WF43 User Manual

Rev 1.1 / 2012-09-18

Widefly Ltd.
http://www.widefly.com

Copyright © 2011 Widefly Limited. All rights reserved.

This User Manual is published by Widefly Limited without any warranty. Improvements and changes to this User Manual necessitated typographical errors, inaccuracies of current information, or improvements to programs and/or equipment, may be made by Widefly Limited any time and without notice. Such changes will, however, be incorporated into new editions of this User Manual.

FCC Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could avoid the users' authority to operate the equipment.

Important Safety Information

PLEASE READ THIS CAREFULLY BEFORE USING WF35 POS PDA

- Always treat your product with care and keep it in a clean and dust-free place
- Do not expose PDA to moisture or humidity
- Do not expose PDA to extreme high or low temperatures
- Do not attempt to disassemble your product
- Use only the chargers and batteries approved by WideFly Limited. The use of any other type may invalidate any approval and warranty. No reverse charging with other chargers, they may have inverse polarity
- Never use the charger if the plug is damaged
- Never touch the charger it your hands/feet are wet
- Do not expose the charger to water, it may cause electrical fires
- Do not repair the charger yourself for your safety
- To reduce the risk of fire or burns, do not disassemble crush or puncture the battery
- Recycle or dispose of the battery safely and properly according to local laws and regulations
- Do not dispose of the battery in fire or water
- Do not let the metal contacts on the battery touch other metal object, it could lead to short-circuit and damage the battery
- Only approval batteries, chargers that are designed for the model can be used with the PDA unit

Document Revision History

To facilitate reading of new or changed content, please see the change mark (vertical line) showing at the left hand side of the paragraphs.

Doc version	Release Date	Author	Major Changes
Rev 1.1	2012-09-18	James	■ Update Chapter 11: System Clone / Backup / Restore
Rev 1.0	2011-10-07	James	■ First release of WF43 user manual, based on major ROM v1.0.2 release.

Contents

Chapter 1: Overview 1

1.1 Front, Rear, Side & Bottom View 1
1.2 LED Status 2
1.3 Loading and Removing Battery 3
1.4 Charging Battery 4
1.5 Power ON / OFF 5
1.6 Suspend (Sleep) / Resume (Wakeup) PDA 7
1.7 Soft Reset (Reboot) by Hardware Reset Key 7
1.8 Clean Reset (Restore to factory default) 8
1.9 Stylus & Screen Calibration 9
1.10 Anti-drop strap, Anti-slip hand strap & Holster 10
1.11 Screen Protectors 12

Chapter 2: System Information 13

2.1 S/N (Serial No.), Memory & Version 13
2.2 Operating System Information 14
2.3 Wi-Fi & Network Information 14

Chapter 3: Admin & User Mode 15

3.1 Introduction 15
3.2 Default Mode 17
3.3 User Mode Restrictions 18
3.4 Customizing Admin / User Mode Shortcuts 18

Chapter 4: Regional Settings 19

4.1 Date & Time Setup 19
4.2 Auto Time Synchronization 20
4.3 Regional Settings 21

Chapter 5: File Explorer 22

5.1 File Explorer 22
5.2 Creating Shortcuts 22

Chapter 6: ActiveSync (PC Synchronization) 23

6.1 Configure ActiveSync via USB 23
6.2 Running ActiveSync via USB 24

Chapter 7: Wi-Fi Settings 25

7.1 Wi-Fi Status and Taskbar Icon 25
7.2 Wi-Fi boot up default state 25
7.3 Single / locked SSID feature 26
7.4 Configure static IP address & DNS 28
7.5 Wi-Fi Seamless Roaming 29
7.6 Always-on W-Fi 31
7.7 WLAN Profile Recovery 32
7.8 Wi-Fi periodic keep-alive 34
7.9 Wi-Fi Auto off and Auto Connection Retry 35
7.10 Notes to Application Developers 36

Chapter 8: Bluetooth 37
8.1 Overall 37

Chapter 9: Power Management 38
9.1 Battery & Charging Status 38
9.2 Dim Backlight Settings 38
9.3 Turn off Screen/LCD, System Sleep & CPU Speed 39
9.4 Sleep Mode Explained 39
9.5 Battery Low 40

Chapter 10: Terminal Services Client / Remote Desktop 41
10.1 Create TSC/RDP Profile 41
10.2 Create RDP shortcut at Today Screen 43
10.3 Serial Port (COM Port) Redirection 43
10.4 Magstripe Card Reader (MSR) 44
10.5 RDP Profile File Format 44
10.6 Common modifications of RDP profile file 46
10.7 Best Practice deploying RDP Application 47

Chapter 11: System Clone / Backup / Restore 48
11.1 Introduction 48
11.2 Local Backup Disk 49
11.3 System Clone / Backup 50
11.4 System Restore 51
11.5 System Restore with WLAN profile Override 52

Chapter 12: Magstripe Card Reader (MSR) 55
12.1 Introduction 55
12.2 Attaching WF43MSR to PDA 56
12.3 Configure MSR by Configuration Utility 57
12.4 Configure MSR sound by WF43 58

12.5 MSR data encryption 59
12.6 MSR data encryption via RDP 59
12.7 Disable Word Completion 60

Chapter 13: Barcode Scanner 61
13.1 Introduction 61
13.2 Configuring Barcode Scanning 62

Chapter 14: Misc. Configurations 63
14.1 Sounds & Notifications 63
14.2 Display & Rotation 63
14.3 Clean Reset 64
14.4 Task Manager 64

Chapter 15: Remote Screen Capture & File Transfer 65
15.1 Remote Display and Screen Capture 65
15.2 Remote File Transfer 66

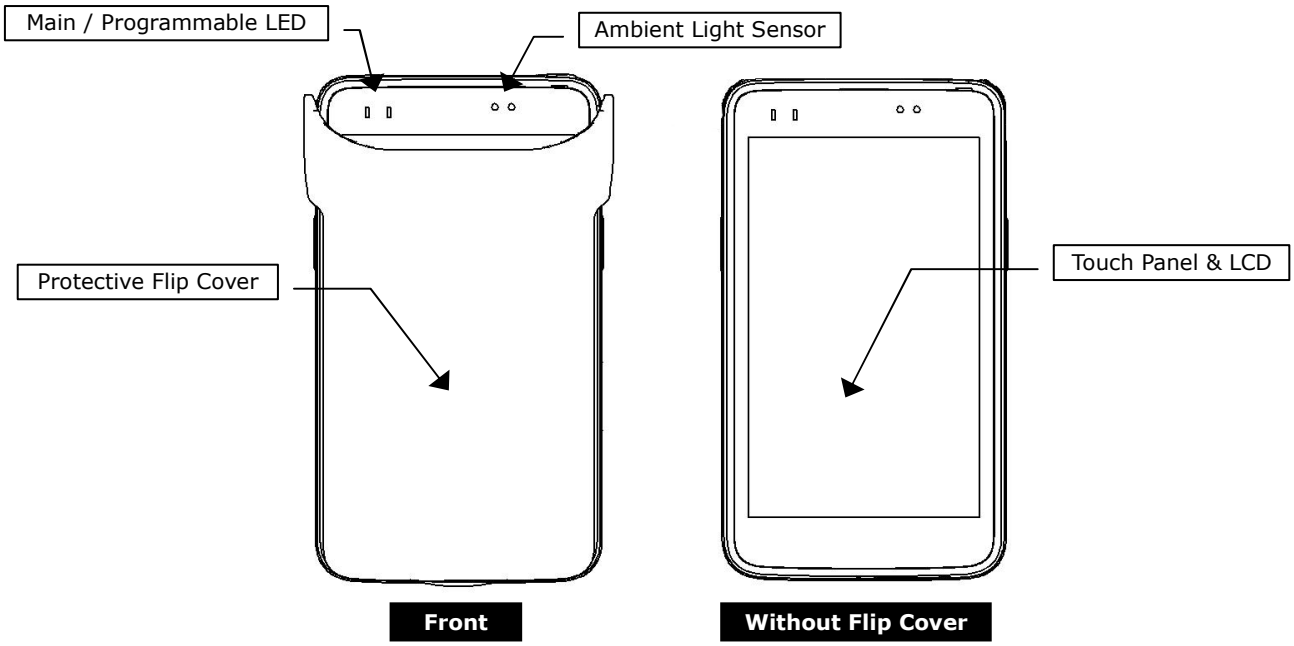
Chapter 16: Configuring Today Screen 67
16.1 Create RDP shortcut on Today Screen 67
16.2 Hide and Show Taskbar 68

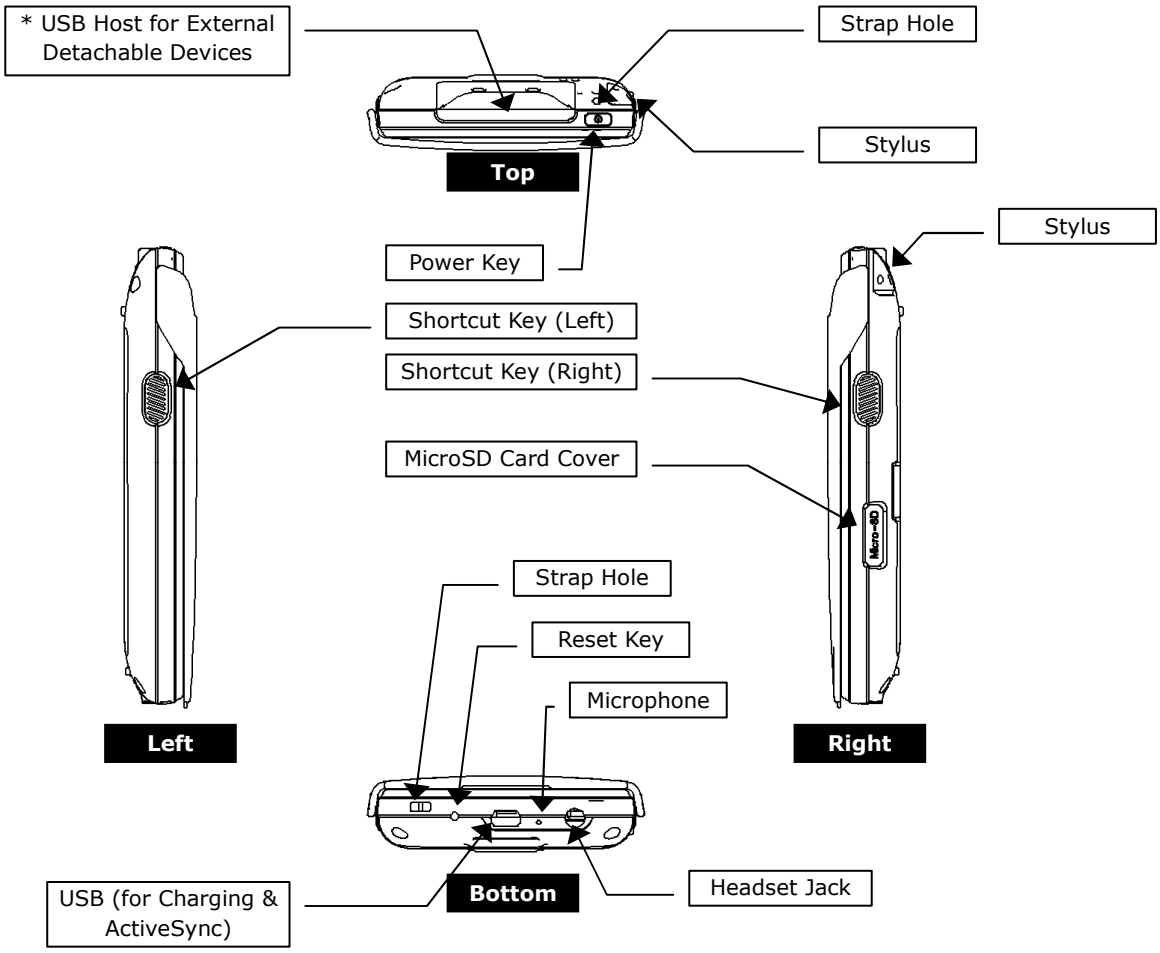
Chapter 17: FTP Download 69
17.1 Introduction 69
17.2 FTP Folders & Files 69

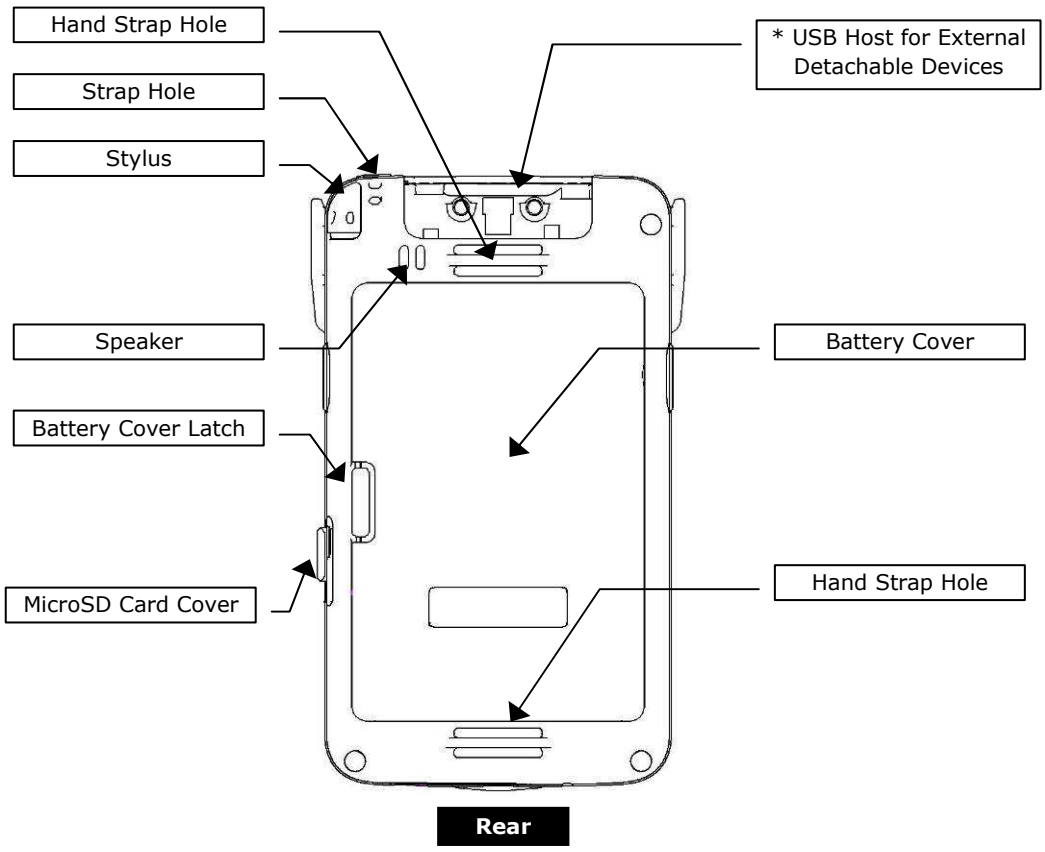
Chapter 18: License Info 70
18.1 Freeware 70

Chapter 1: Overview

1.1 Front, Rear, Side & Bottom View







***For example:** MSR (Magstripe Card Reader), Laser Barcode Scanner, RFID Reader

1.2 LED Status

Power / Main LED (left) indicates Wi-Fi & battery status.

LED status	Descriptions
Red flash	Battery low
Red solid	Battery very low (will auto off PDA soon)
Amber flash	Battery charging
Green solid	Battery full
Blue flash (quickly)	Wi-Fi searching
Blue flash (slowly)	Wi-Fi connected
Off	Wi-Fi disconnected / Wi-Fi auto off status

1.3 Loading and Removing Battery

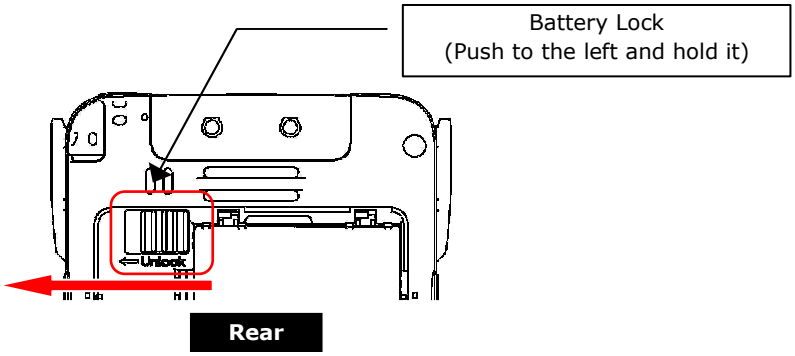
Loading Battery

1. Align the battery metal contacts with the contacts inside the battery compartment.
2. Press the battery downwards until it fits the battery compartment. Push the battery until it is locked automatically.

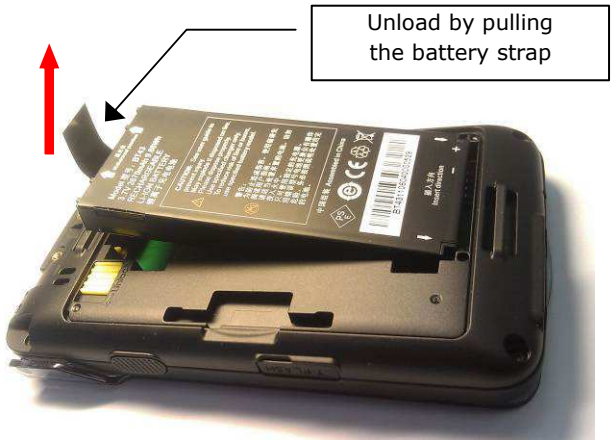
Removing Battery

1. Turn off the PDA by press-and-holding the power key for 1 second. Press "OK" on the "Power off" dialog box.

2. Open the battery cover. Push the battery lock to the left and hold it.



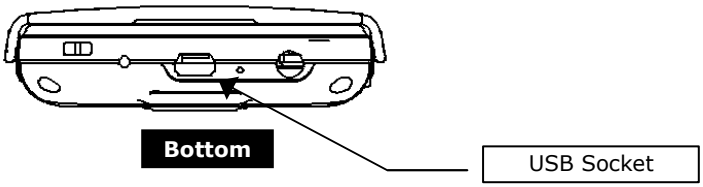
3. Gently lift the battery by pulling the strap attached to the battery top position.



1.4 Charging Battery

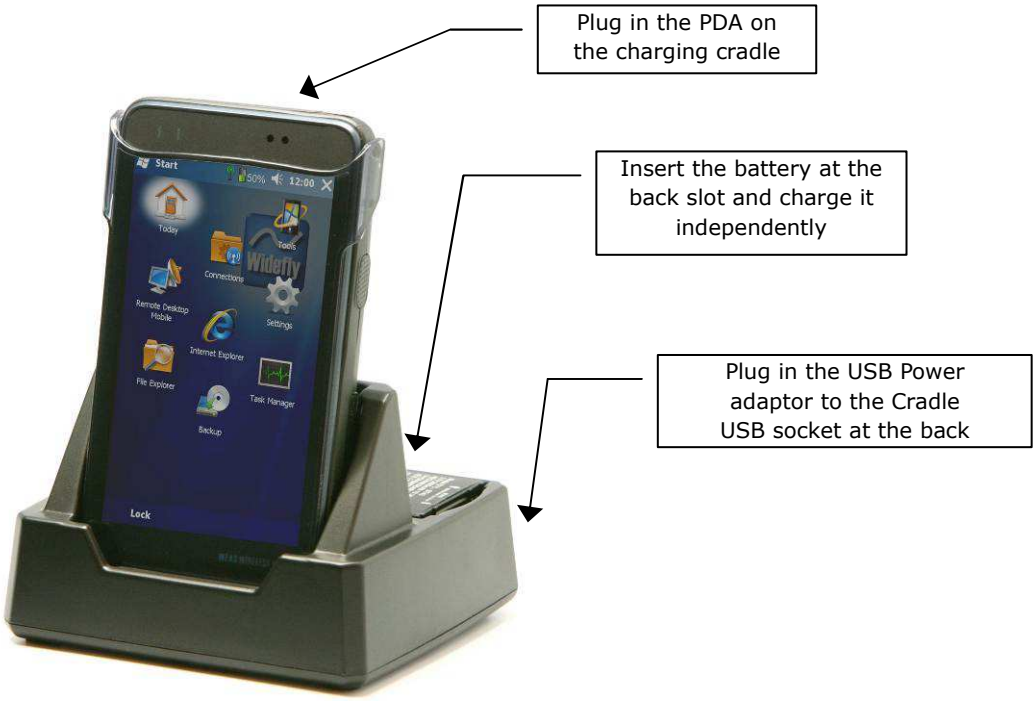
Charging by USB Power Adaptor

Plug in the USB power adaptor to PDA's bottom USB socket.



Charging by Cradle

WF43 Charging Cradle (Item code: WF43CC) is an optional accessory that is able to charge WF43 as well as an independent battery simultaneously.


Plug in the PDA on the charging cradle
Insert the battery at the back slot and charge it independently
Plug in the USB Power adaptor to the Cradle USB socket at the back

NOTE: PDA's USB socket was loaded with 5V⎓(DC), 500mA during normal condition.

.

DO NOT uses the power adaptor other than the one provided by Widefly or warranty will be voided. Most consumer USB power adaptors DO NOT have sufficient power rating as well as protection circuitry to support charging PDA & extra battery via cradle.

1.5 Power ON / OFF

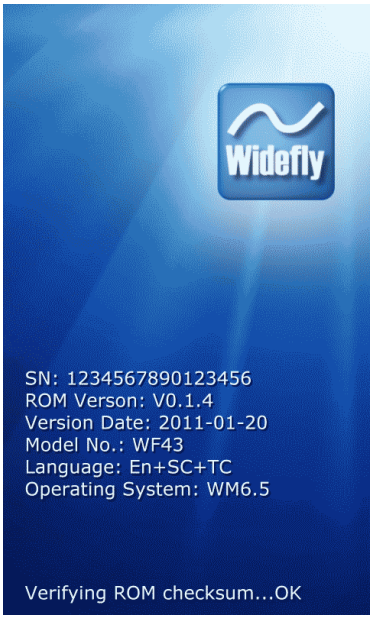
Power ON

Battery Level Very Low
To bootup the system, it requires Initial Charging for 10 to 15mins.
Please plug in the power adaptor to perform battery charging or Change a new battery.

To power on the PDA, press and hold the power key for 1 second. When there is green LED, the unit is ready to boot up to the operating system.

However, if the LED is **RED (or no LED light)**, battery level is very low and is insufficient to boot up the unit. A warning screen will be displayed.

To restore to the minimum required power, charge up the unit for 10 to 15 minutes.



Normal boot up screen displays system info below:

- Serial No. (SN), a globally unique no. to identify a PDA
- ROM Version and Version Date
- Model No.
- Language (e.g. EN is English version, EN+SC is English + Simplified Chinese version)
- Operating System: WM6.5
- The "Verifying ROM checksum…" should display OK or else the system could not be loaded properly. In that case, re-flashing of ROM is required.

Power OFF

To power off the PDA, press-n-hold the power key for 1 second. System will pop up a dialog box "Power off". Press OK to confirm system shutdown.

1.6 Suspend (Sleep) / Resume (Wakeup) PDA

PDA can be suspended like sleeping, called "sleep mode" to achieve maximum power saving. When PDA is in sleep mode, the LCD backlight and touch panel are off, CPU is in sleeping status while Wi-Fi can be kept connected.

- To force sleeping (suspend) of the PDA manually, lightly press the power key.
- To wake up (resume) PDA manually, lightly press the power key again. Once woken up, PDA is back to the original status with the LCD backlight on and CPU running.

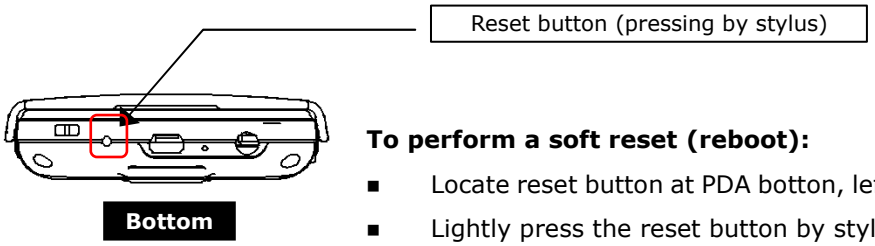
NOTE: Please refer to "Chapter 9: Power Management" for power settings.

"Sleep Mode" is a unique Widefly feature that allows maximum power saving yet Wi-Fi connection could be kept online.

1.7 Soft Reset (Reboot) by Hardware Reset Key

Soft reset may be necessary in case system does not response any button & screen contacts. The soft reset is like a reboot of the system. It does not erase any installed programs or saved data.

Always save the data within the active programs running on PDA before performing a soft reset or unsaved data may be discarded.



To perform a soft reset (reboot):

- Locate reset button at PDA botton, left to the USB socket
- Lightly press the reset button by stylus
- System will be rebooted

Note: "soft reset" is a force reboot of system. It discards all recent changes of system settings or file content that are pending for flushing to the physical flash memory.

Always use "Power off" (press-and-hold power key) to turn off the PDA or recent changes of system settings / registry may not be saved to the file system.

1.8 Clean Reset (Restore to factory default)

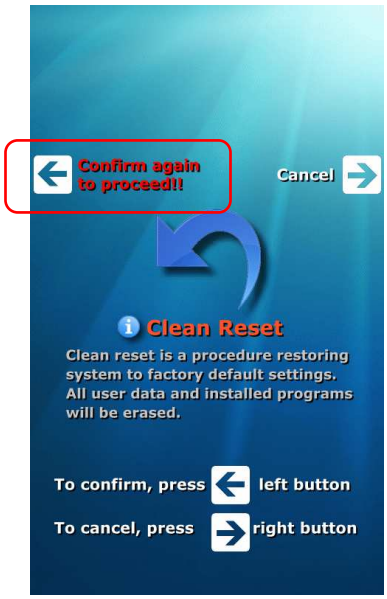
In case a thorough reset of PDA is required, clean reset can be performed to erase all installed programs, settings and data. The clean reset is equivalent to restoring system to factory default.

To perform a clean reset:

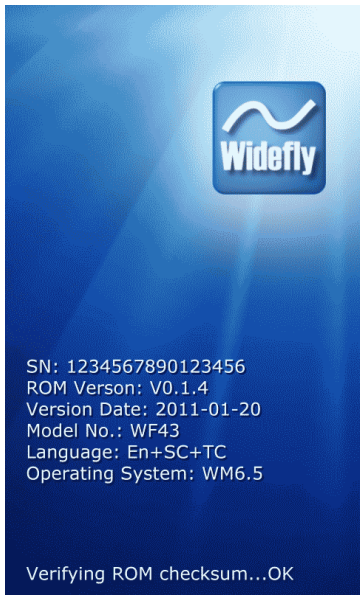
- Turn off the PDA (press-and-hold the power key and select "Power Off")
- Press-and-hold PDA's right shortcut key (keep holding)
- Press the power key to boot up the unit.
- Keep holding the right shortcut key until "Clean Reset" screen is seen. Follow the screens below:

Confirm
Cancel
Clean Reset
Clean reset is a procedure restoring system to factory default settings. All user data and installed programs will be erased.
To confirm, press left button
To cancel, press right button

"Clean Reset" screen


Confirm again to proceed!!
Cancel
Clean Reset
Clean reset is a procedure restoring system to factory default settings. All user data and installed programs will be erased.
To confirm, press left button
To cancel, press right button

Press left shortcut key twice to confirm clean reset



Subsequent reboot will restore PDA to factory default settings

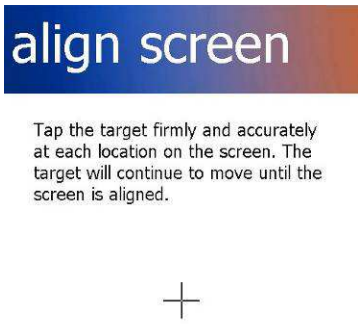
Note: clean reset could also be performed via Windows Mobile environment. Please refer to Chapter 14.3 – Clean Reset.

"Clean reset" is a process to restore system to factory default. All installed programs and data will be erased.

1.9 Stylus & Screen Calibration

In case touch screen could not respond to tapping positions on screen accurately, recalibration may be necessary. Click **Start > Settings > Screen**

Tap "Align Screen"


align screen
Tap the target firmly and accurately at each location on the screen. The target will continue to move until the screen is aligned.

Follow targets and tap the screen by stylus

1.10 Anti-drop strap, Anti-slip hand strap & Holster

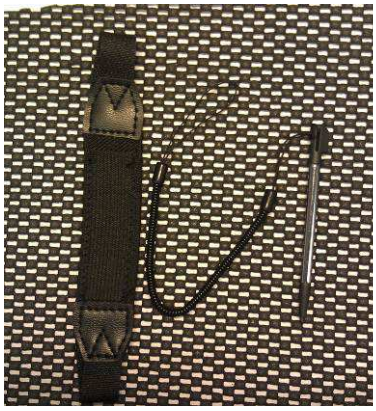
Standard PDA package comes with anti-drop elastic strap and anti-slip hand strap. Anti-drop strap is a proven and effective solution to help protect PDA from damaging when the unit drops to the ground.

Anti-drop strap

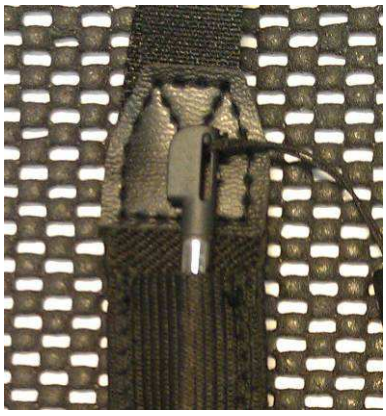
- The anti-drop strap attaches to PDA bottom strap hole
- The other end of the strap is a lock, designed to attach to user's belt position
- The middle part of the strap is an elastic spring that is able to absorb the force when the PDA unit is hitting the ground or when PDA is out of users' hands

- A detachable design to facilitate users to return the PDA units to their supervisors / managers

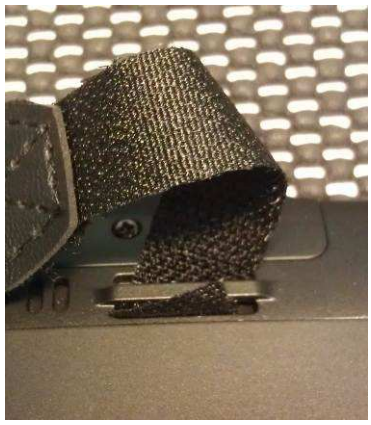
Anti-slip hand strap & Tethered Stylus



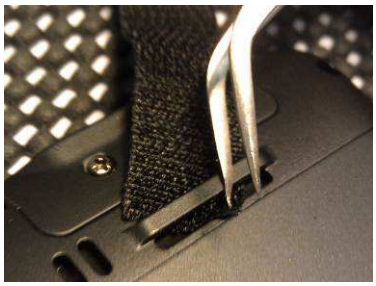
Hand strap & tethered stylus. This is an extra stylus longer than the PDA's one.



The tethered stylus could be inserted and held by the hand strap.



To insert hand strap, remove the tethered stylus first. Curve the one corner of the strap and insert into the strap hole.



Use sharp pliers to pull it out of the strap hole further

Adjust the length by affixing the hook-and-loop position

Hand strap attached. Anti-drop strap could be used together

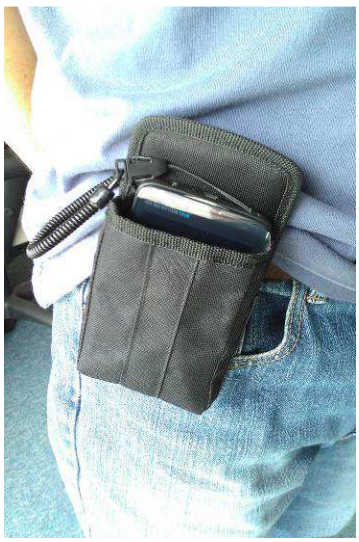
The tethered stylus could be held by the middle of the hand strap

It is site proven that anti-drop elastic strap helps reduce damaging of PDA effectively.

Holster

Holster is an optional accessory to facilitate holding of PDA from the waiter/waitress belt position. The holster is designed to use with anti-drop as well as hand strap altogether.

Holster clipped at belt position



PDA in inserted to the holster upside down. To further protect the unit, anti-drop strap is used.

The unit is taken out from the holster naturally.

1.11 Screen Protectors

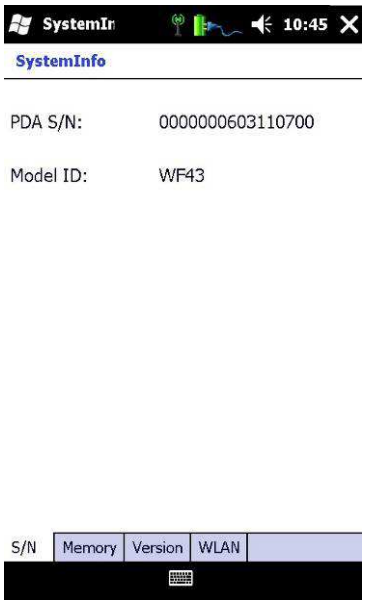
Each standard package comes with a piece of screen protector film. The film helps protect touch screen from scratches, tears, dirt, dust, oil and grease effectively.

Screen protector film is a highly recommended accessory to help protect touch screen from wear & tear.

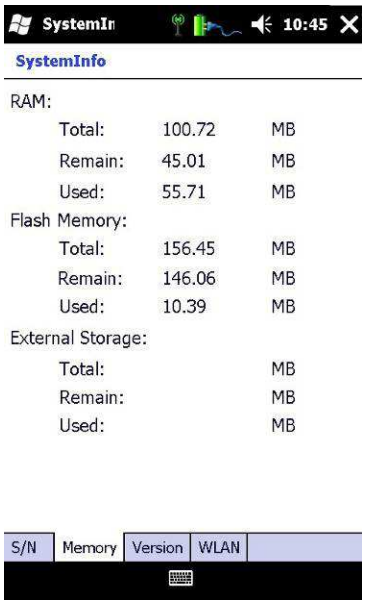
Chapter 2: System Information

2.1 S/N (Serial No.), Memory & Version

System information provides important information for deployment and ongoing support. To access the info, tap **Start > Settings > System Info**

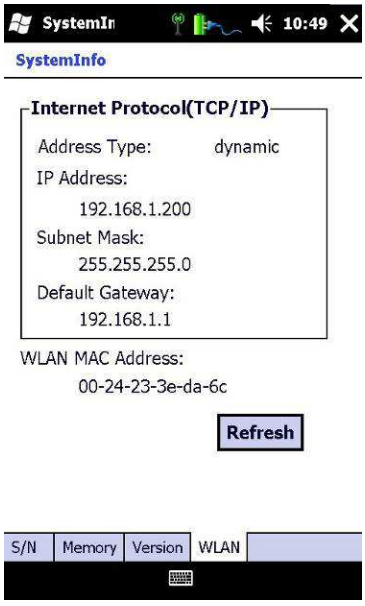


- S/N is a globally unique serial no. to identify a PDA



- Memory info

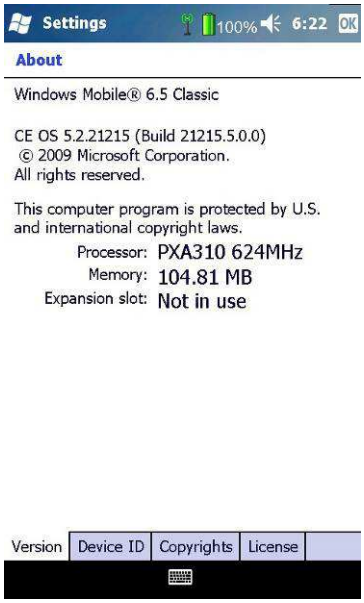
- ROM version info



- WLAN info

2.2 Operating System Information

Operating system information is shown at **Start > Settings > Others > About**



Operating System info

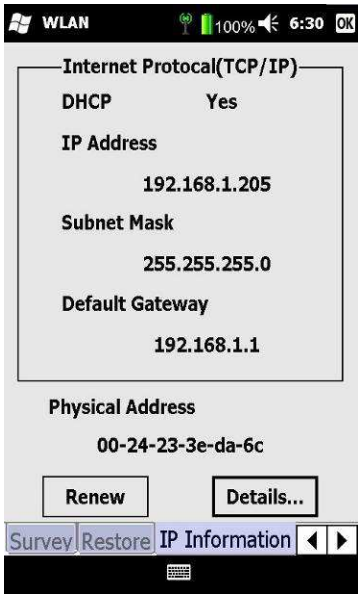
Settings
100% 6:23 OK
About
Your device uses this information to identify itself to other computers. Enter a name that starts with a letter and contains the characters _, A-Z, or 0-9.
Device name: WF43
Description:
Version
Device ID
Copyrights
License

Device ID info. Default ID is WF43

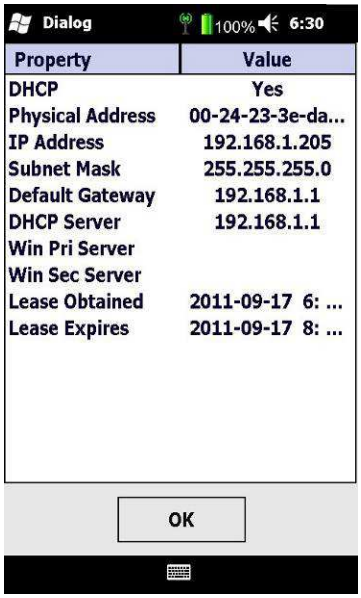
License info

2.3 Wi-Fi & Network Information

Wi-Fi and network information provides important information for network configuration. Tap Wi-Fi icon or tap **Start > Settings > Wi-Fi > IP Information (tab page)**



IP address info



Detail IP address info, e.g. DHCP Server, DHCP lease time

Chapter 3: Admin & User Mode

3.1 Introduction

WF43 PDA has two distinct modes of operation: Admin Mode and User Mode.
In Administrator Mode, system administrators or field service technicians have full rights to configure system settings and install / un-install applications. This is a mode typically used for initial stage of setup and ongoing maintenance.

User Mode, as its name implies, is specially designed for end users who use the PDA as a dedicated working terminal or appliance. Since system configurations are completely hidden in user mode, e.g. IP address, Wi-Fi keys, application shortcuts & etc, system integrators (SIs) would find deploying WF43 solutions much fewer support calls in compare with deploying consumer based PDAs. Since users have no way to access to file system in this mode, no files or local database can be tampered or taken out of the device. Therefore, data security could be enforced effortlessly.

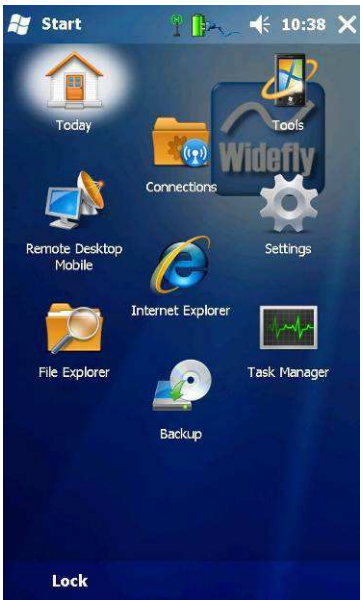
The Start Menu shortcuts could be customized independently in Administrator Mode and User Mode. Standard control panel features in admin mode are reduced in user mode.

The characteristics of the Administrator Mode and User Mode are summarized in below table:

Mode	Description
Administrator Mode	■ An operating mode for administrators & System integrators. ■ Full administrative rights in major system configurations: 1. Network settings, e.g. Wi-Fi profile settings 2. Program installation / un-installation 3. File manager for file, folder, shortcuts access 4. Driver / OS update 5. System backup & restore
User Mode	■ An operating mode for end users or operators in production site. ■ The PDA works like a kiosk. Only designated applications (via shortcuts) are allowed to execute. ■ Access to system configuration is prohibited

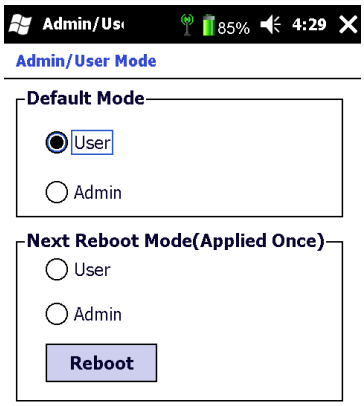
User mode enables zero support of the PDA because all system settings are hidden from the end users.

The following are screen captures for comparing administrator & user mode. In user mode, only limited set of control panel features are available.

Administrator Mode	User Mode
	
■ Full items in start menu	■ Configurable items in start menu (default is empty except Today & Settings shortcut)
■ Full features in Start > Settings	■ Limited features in Start > Settings Note: ■ In user mode, features are further restricted by hiding some tab pages of settings. ■ For example, WLAN panel in user mode has no "Advanced" tab page to configure settings.

3.2 Default Mode

A brand new PDA is pre-configured to run as Administrator Mode. All features can be accessed without restrictions. To configure default boot up mode (Admin or User), goto **Start > Settings > User/Admin Mode**.



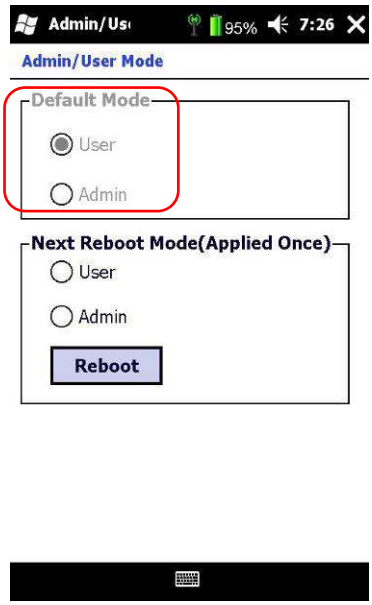
Change to User Mode (under Admin Mode)

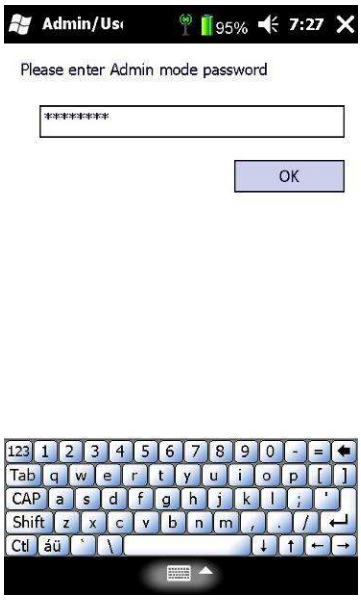
To change to "User Mode", simply select "User" and press "Reboot".

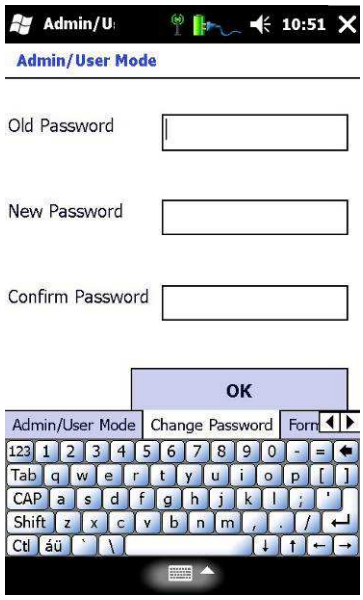
Note:

- To apply change of default mode, system reboot is required.
- Under Admin mode, no password is required for changing to user mode.

Change to Admin Mode (under User Mode)







End users cannot break the user mode restrictions and thus "Default Mode" options are greyed out.

For administrators, they could select "Next Reboot" option as "Admin" and press "Reboot". This triggers reboot of system into Admin mode but not changing the original default user mode. However, password is required (Default password is 12345678). Admin mode password should be changed when PDAs are deployed to production environment.

3.3 User Mode Restrictions

The following table summarizes the restrictions in user mode.

Items	Purpose
System settings change (Most are features of control panel)	■ No changes of environment pre-configured by administrator ■ No support due to accidentally changes of settings
Application shortcut change (Start Menu shortcuts)	■ No changes of application environment
Program installation / un-installation	■ No installation of unauthorized applications, e.g. games, personal utilities ■ No removal of pre-configured applications & runtime libraries
Direct access to files & local databases (via File Manager)	■ No unauthorized access to files & database ■ No copying of data out of PDA ■ No program installation via SD card Note: Administrator should not create shortcut to file manager in user mode
ActiveSync connection	■ Prevent unauthorized installation / un-installation of applications ■ Prevent direct access to files, local database & setting systems

3.4 Customizing Admin / User Mode Shortcuts

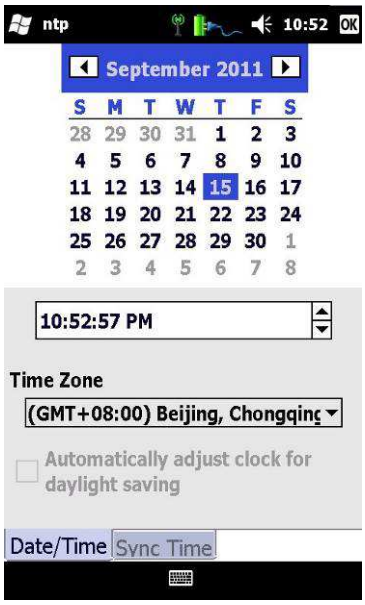
Program shortcuts shown **Start Menu** can be customized independently in admin & user mode. Typically, user mode may contain only one or two application shortcuts.

Shortcuts	Admin Mode	User Mode
Start Menu	\Windows\Start Menu\Programs	\Windows\menu_eng_user\Programs

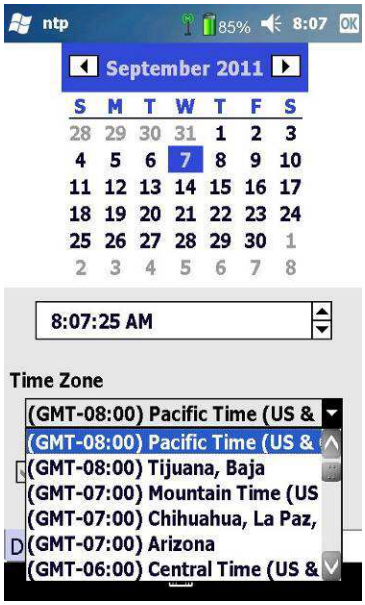
Chapter 4: Regional Settings

4.1 Date & Time Setup

To change date/time and time zone, double tap the Windows taskbar Real Time Clock (e.g.) or tap **Start > Settings > Others > NTP**


ntp
10:52
OK
September 2011
S M T W T F S
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 1
2 3 4 5 6 7 8
10:52:57 PM
Time Zone
(GMT+08:00) Beijing, Chongqing
Automatically adjust clock for daylight saving
Date/Time
Sync Time

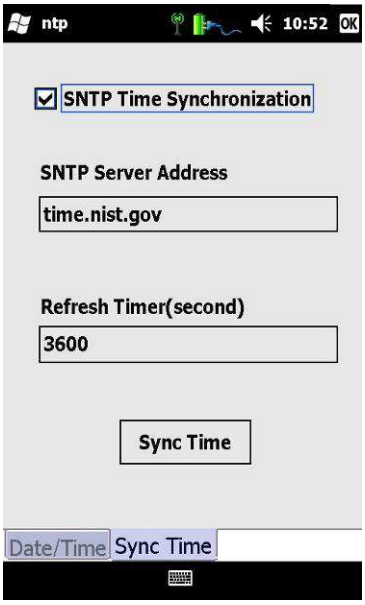
- Adjust date & time


ntp
85%
8:07
OK
September 2011
S M T W T F S
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 1
2 3 4 5 6 7 8
8:07:25 AM
Time Zone
(GMT-08:00) Pacific Time (US &
(GMT-08:00) Pacific Time (US &
(GMT-08:00) Tijuana, Baja
(GMT-07:00) Mountain Time (US
(GMT-07:00) Chihuahua, La Paz,
(GMT-07:00) Arizona
(GMT-06:00) Central Time (US &

- Time zone must be properly configured if "Time Sync" is used. Otherwise, system could not display correct time according to local time zone setting.

4.2 Auto Time Synchronization

The "Time Sync" feature enables auto time synchronization with any time server supporting Simple Network Time Protocol (SNTP) on the network via Wi-Fi connection. Tap **Start > Settings > Others > NTP (Time Sync tab page)**



By default, the SNTP Time Sync function is enabled.

- To enable/disable the Time Sync function, tap to check/uncheck the "SNTP Time Synchronization" checkbox.
- The default SNTP server is **time.nist.gov**.
- System integrator could configure a POS server with SNTP service for synchronizing date/time to all PDAs. In that case, SNTP server address could be IP address like 192.168.x.y.
- Default Time Sync refresh period is 3600 seconds (i.e. 60 minutes).
- Tap the "Sync Time" button to manually perform a Time Sync operation immediately. (Remember to set the correct a time zone)

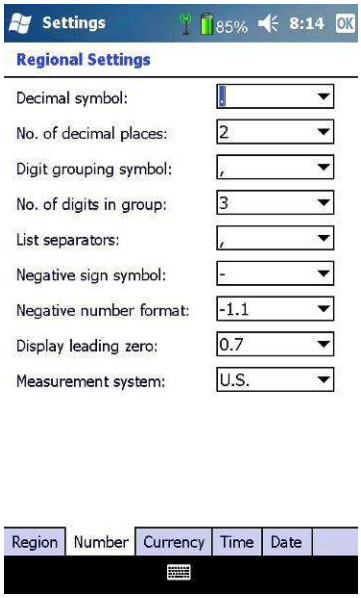
NOTE:

- Time sync is disabled in sleep mode. Next time sync attempt will be deferred when PDA is manually woken up.

4.3 Regional Settings

Regional settings like date & time format, number and currency format can be configured in **Start > Settings > Input & Languages > Regional Settings.**

Region tab page



Number format tab page

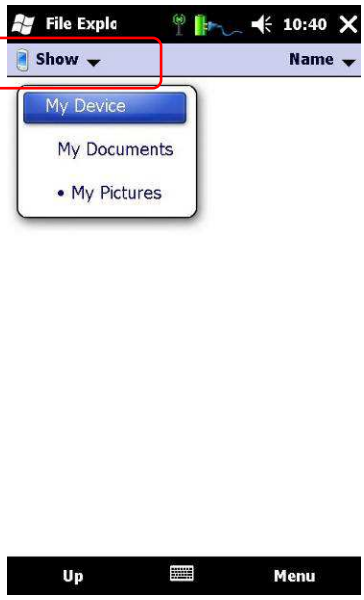
Time format tab page

Chapter 5: File Explorer

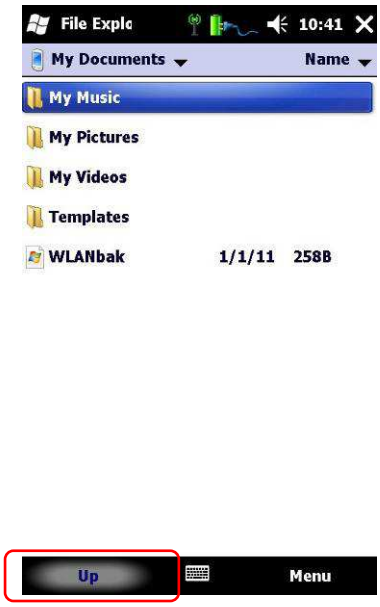
5.1 File Explorer

File Explorer is one of most frequently used tool. It provides all basic file operations like copy, cut, paste, paste shortcut, delete & etc.

Start > File Explorer



Tap top left folder selector to jump to parent folders.



To jump to immediate parent folder, simply tap the bottom left "Up" label.

5.2 Creating Shortcuts

There are two ways to create a shortcut: "Copy & Paste Shortcut" using File Explorer and ActiveSync. The following is an example using File Explorer.

Tap-and-hold the file and "Copy"

Tap-and-hold to "Paste Shortcut"

Shortcut created

Chapter 6: ActiveSync (PC Synchronization)

Microsoft ActiveSync is software that allows user to synchronize Windows Mobile or Windows CE-based devices with a Windows-based PC.

If a PC is running Windows Vista/7, ActiveSync is managed through the Windows Mobile Device Center. For earlier versions of Windows, Microsoft ActiveSync is needed to be installed. The Microsoft ActiveSync 4.5 is recommended for installation.

The ActiveSync enables files browsing, applications installation/removal.

6.1 Configure ActiveSync via USB

By default, the PDA uses the USB port for the PC connection to ActiveSync. User may double check the status on **Start > Connections > "USB to PC" and "ActiveSync"**

Windows XP Professional is used for illustration purpose. Make sure ActiveSync (or Windows Mobile Device Centre) is properly installed.

- Right click ActiveSync tray icon in the Windows taskbar
- Select "Connection Settings…" from the pop up menu.
- Enable the "Allow USB connections" checkbox option

6.2 Running ActiveSync via USB

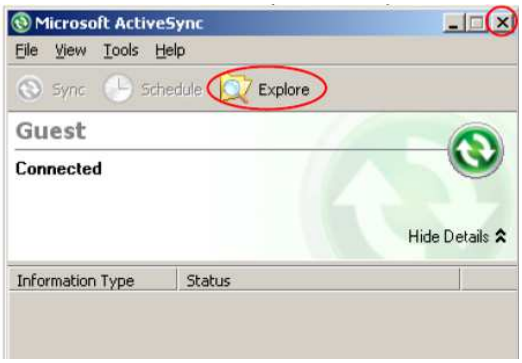
Make sure PDA is under admin mode (since USB is disabled in User mode by design for security purpose).

Connect PDA to PC via mini-USB cable. PC's ActiveSync will be started automatically.

- The ActiveSync tray icon will changes from grey to green
- The ActiveSync startup dialog appears. Select "No" and press "Next"

New Partnership
Set Up a Partnership
Before you can synchronize information between your mobile device and this computer, you must set up a partnership between them.
Would you like to set up a partnership?
Yes
Set up a partnership so that I can synchronize information between my device and this computer.
No
I don't want to synchronize information. Set up my device as a guest so that I can copy or move information between my device and this computer.
< Back
Next >
Cancel
Help

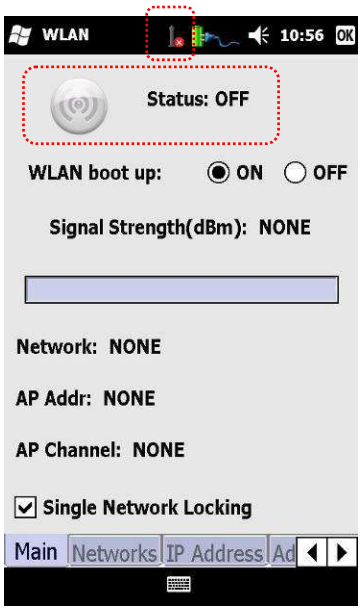
- Press "Explore" to browse the files and folders of the PDA remotely



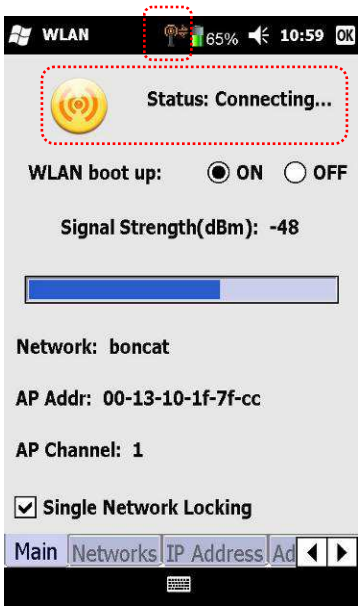
Chapter 7: Wi-Fi Settings

7.1 Wi-Fi Status and Taskbar Icon

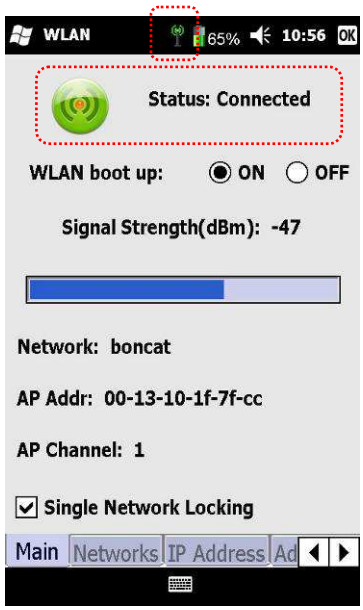
Tap WLAN icon on the status bar or tap **Start > Settings > Wi-Fi** to open WLAN panel. Tap the Wi-Fi on/off button to manually turn on or off the Wi-Fi. The connected network name (SSID), MAC address, signal strength, .channel, etc are shown in the main page



- WLAN is off
- WLAN icon: grey with red cross
- Wi-Fi LED: off

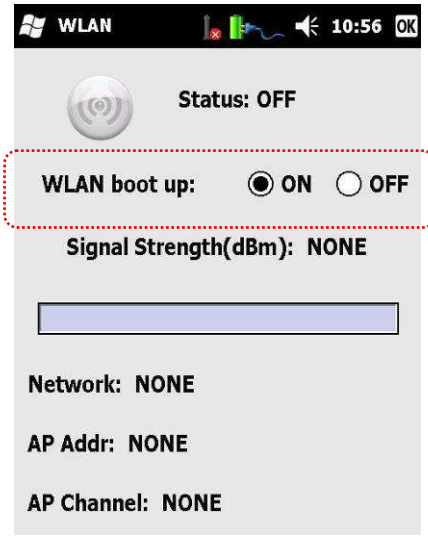


- Tap WLAN button to turn it on
- Wi-Fi is searching for networks (access points)
- Wi-Fi icon: amber
- Wi-Fi LED: blue flash (quick)



- Wi-Fi connected to a access point
- Wi-Fi icon: green
- Wi-Fi LED: blue flash (slow)

7.2 Wi-Fi boot up default state



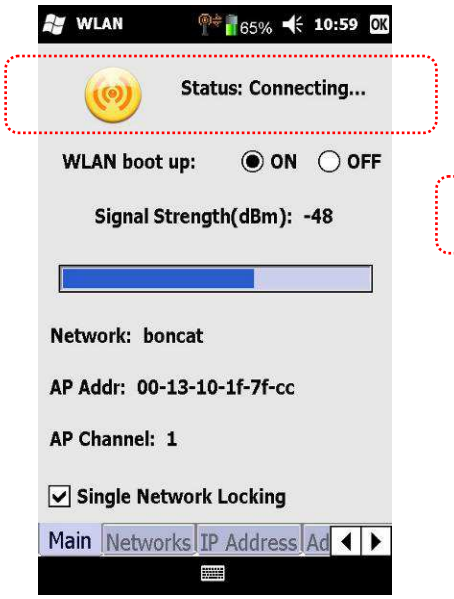
By default, Wi-Fi is turned on after system boot up.

For offline application, Wi-Fi default state could be configured as "off"

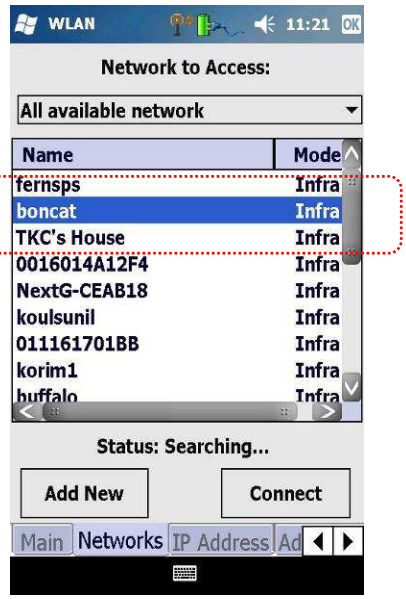
Note:
WLAN last on/off state is not remembered in the system. The behavior follows the settings in this option.

7.3 Single / locked SSID feature

Single / locked SSID is a special feature to lock to a designated network (i.e Access Points with the same SSID). This ensures users will not accidentally connect to nearby access points (APs) and cause interruption of POS application and support calls.

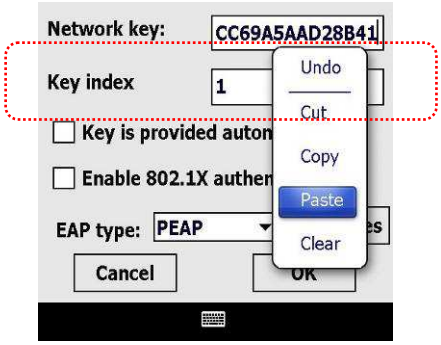


- Tap WLAN on/off button to turn on Wi-Fi
- Tap "Networks" page



- Wi-Fi displays all available networks*.
- Double tap a network name to start configuring it
- For hidden network, tap "Add New" to add a profile manually

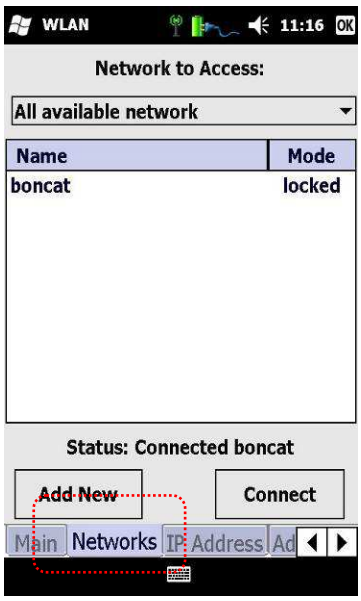
- Enter security info, for example Authentication, Encryption and etc.



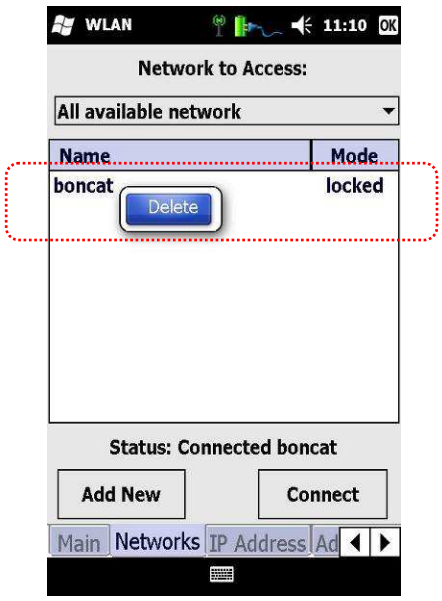
- Tips: Since network key can be as long as 26 characters (WEP 128-bit key). Such key could be copied and pasted from text editor.
- To paste, tap-and-hold the input field of network key. Select "Paste" in the popup menu
  Text editor is located at **Start > Tools > lgtEditor**

*** Note:** A Wi-Fi access point can be configured to broadcast or hide its SSID. Only networks with broadcasting SSID can be searched and seen in the list.

Delete a SSID profile



- To delete a SSID profile, goto "Networks" page

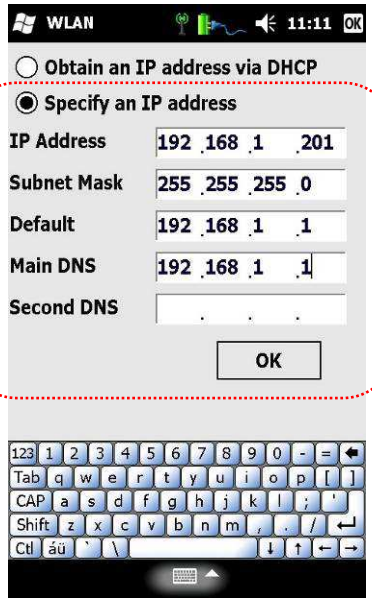


- Press-and-hold the SSID
- Select "delete" from the popup menu

"Single / locked SSID" feature ensures that PDA only connects to designated network

7.4 Configure static IP address & DNS

Tap WLAN tray icon or tap **Start > Settings >Wi-Fi** and select the IP Address (tab page) to define the static IP and DNS



- Define static IP address
- Always input default "Default Gateway". See note below

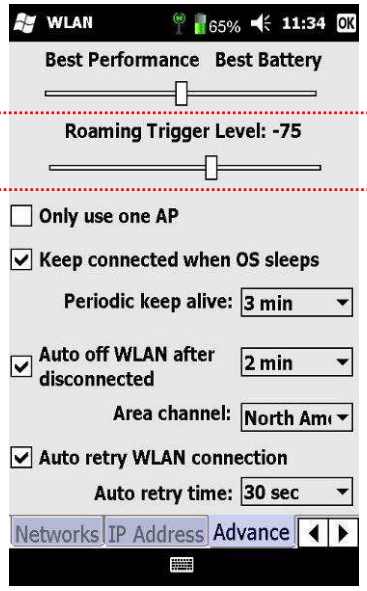
Important Note: Always define "Default Gateway". Wi-Fi module has a special mechanism to maximize Wi-Fi seamless roaming across access points. If your network does not has a network router, default gateway could be pointed to POS server or any network equipment that could respond to TCP/IP traffic.

Always define "Default Gateway" as it is required for seamless roaming

7.5 Wi-Fi Seamless Roaming

Wi-Fi reliability lies in the ability and performance of Wi-Fi seamless roaming. With the enhanced WLAN driver and firmware by Widefly, PDA could typically roam across access points (with same SSID) less than a second. The PDA provides genuine roaming, which online applications is transparent to the roaming process while the network session (TCP/IP) could be maintained. This ensures no interruption to real-time POS applications.

To configure Wi-Fi roaming, tap **Start > Settings > Wi-Fi > Advance (Tab page)**

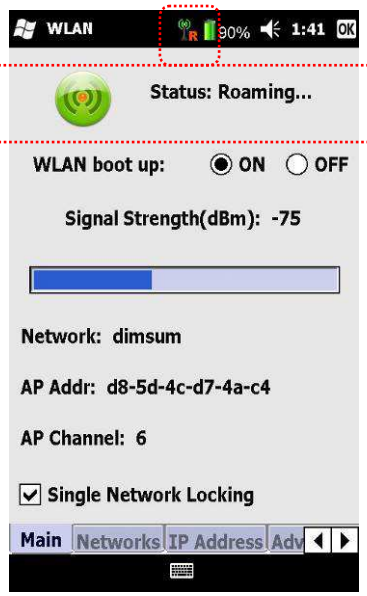


Multiple Access Points (AP) Environment

For multiple APs site, it is important to perform wireless site survey to figure out the best placement of access points in order to provide the best coverage of wireless signal with the least signal interference.

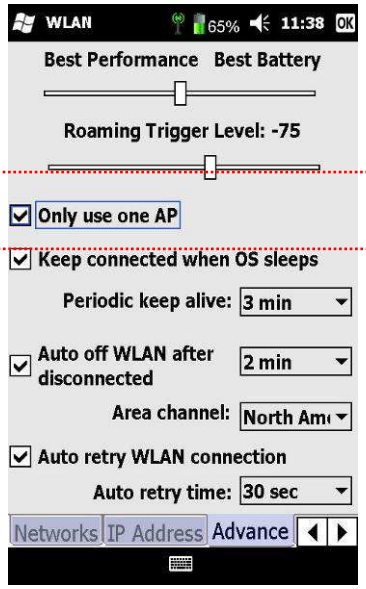
Roaming Trigger Level "-75dBm" is an optimal value for most environments. The mechanism works like below:

- When the signal strength of a Wi-Fi connection becomes weak and beyond roaming trigger level, Wi-Fi will search for nearby APs in background transparent to users. The searching will not impact existing Wi-Fi connection.
- In this status, a "R" will be added on top of the Wi-Fi icon. This "R" indicates background searching for AP. The Wi-Fi status will be displayed as "Roaming".
- If an AP could be searched with signal strength better than 10dBm of the trigger level, i.e. -65dBm if -75dBm is the trigger level. Wi-Fi will roam to this AP automatically.



Note:

Roaming trigger level is also a key performance meter to the wireless site survey. For example, -75dBm is equivalent to a performance level that in every single location of a wireless site, there should be one AP providing signal strength -75dBm or better. If APs are placed with the least interference (e.g. adjacent channel 1, 6, 11) and they have fully covered the site, seamless roaming could be achieved easily.



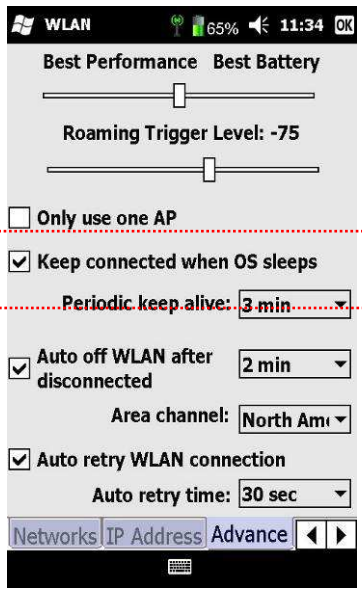
Single Access Point Environment

For single AP site, since there is no more access point with stronger signal that would be roamed, selecting "Only use one AP" will be optimal. This will disable system from searching for nearby access point and thus will save power.

To apply change of this option, restart of Wi-Fi is required (i.e. tap the Wi-Fi button OFF and then ON again).

For detail tips and tricks of deploying multiple APs in a wireless site, please refer to the document "Best Practices for Deployment Widefly POS PDA - Wireless Site Planning & Implementation"

7.6 Always-on W-Fi



Wi-Fi remains connected in "Sleep mode"

"Always-on Wi-Fi" is a unique feature of Widefly solution. This is a design to Keep Wi-Fi connected even PDA is in sleep mode. By default, it is turned on. See checkbox "Keep connected when OS sleeps"

When PDA enters "sleep mode", touch screen and LCD are off, CPU is in sleeping status for maximum power saving while Wi-Fi connection is kept connected.

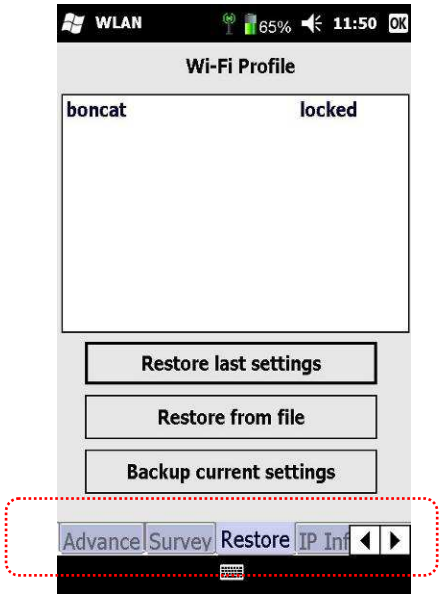
In "sleep mode", pressing the power key will wake up the PDA manually. Online POS application could transmit data to POS server as long as PDA has woken up without any delay re-connecting to network.

If "Always-on Wi-Fi" is disabled, it could achieve maximum power saving in "sleep mode". However, it will take 5 to 10 seconds to re-connect to AP if PDA is woken up manually. This may defeat the key requirement of the always-on Wi-Fi connectivity of a POS application.

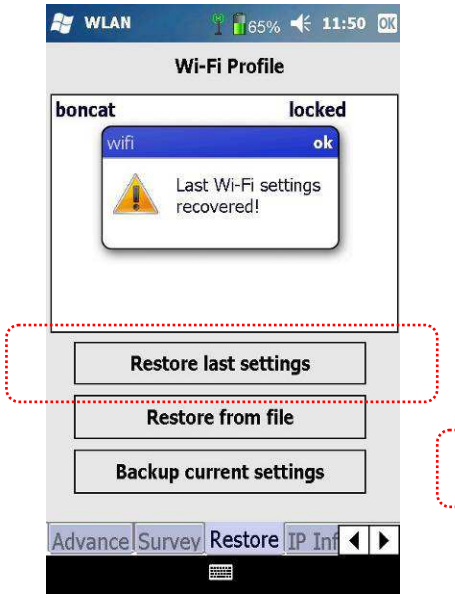
7.7 WLAN Profile Recovery

If Wi-Fi may not function properly, e.g. SSID is lost because of registry corruption, the recovery function allows restoration of the last-known-good WLAN profile.

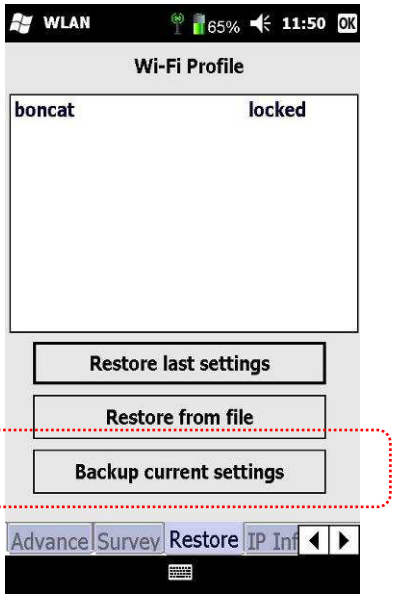
This feature reduces potential support due to abnormal Wi-Fi behavior in case of system registry issue.



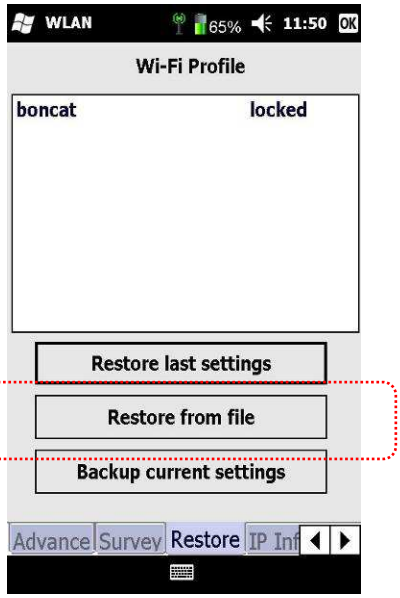
- Tap "Restore" page



- Press "Restore last settings" will restore last known good Wi-Fi profile



- Existing Wi-Fi profile could be saved by pressing "Backup current settings" in INI file format.



- Wi-Fi profile could be restored from a file
-
-

File format – WLAN.ini

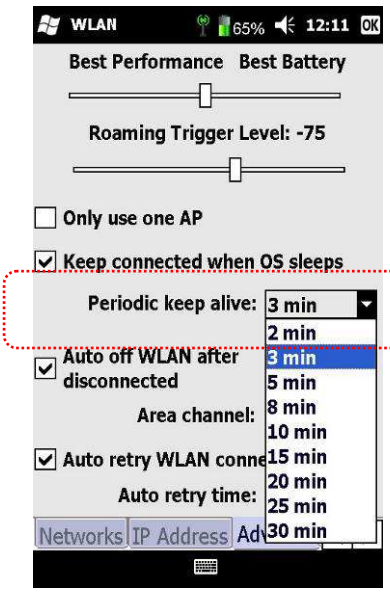
The following is a WLAN.ini file that could be used for restoring specific WLAN & IP address info.

```
DHCP=0                          ← 0: Fixed IP / 1:DHCP
IP Address=192.168.18.51        ← For fixed IP, the assigned IP address
Subnet Mask=255.255.255.0       ← For fixed IP, the subnet mask
Default Gateway=192.168.18.1    ← For fixed IP, the default gateway
Primary DNS=192.168.18.1        ← For fixed IP, the primary DNS
Second DNS=                     ← For fixed IP, the secondary DNS
Primary WINS=                   ← For fixed IP, the primary WINS
Second WINS=                    ← For fixed IP, the secondary WINS

SSID=WFWEP              ← SSID of the Wi-Fi network
NetworkType=1           ← 1: AP mode
SecurityType=1          ← 0: Open / 1:Shared / 4: WPA-PSK / 7: WPA2-PSK
EncryptionType=1        ← 0: WEP / 4: TKIP / 6: AES
Networkkey=1234567890   ← clear text network key **
NetworkkeyBin=          ← encrypted network key generated by the WLAN panel
WEPKeyIndex=1           ← WEP key index.  Most often is 1
SingleNetwork=1         ← 1: single SSID
```

** **Note:** clear text network always overrides binary encrypted network key

7.8 Wi-Fi periodic keep-alive



Periodic keep-alive

There is common that access points would kill Wi-Fi connection session if it has been idle for few minutes. This causes issue to application requiring always-on Wi-Fi.

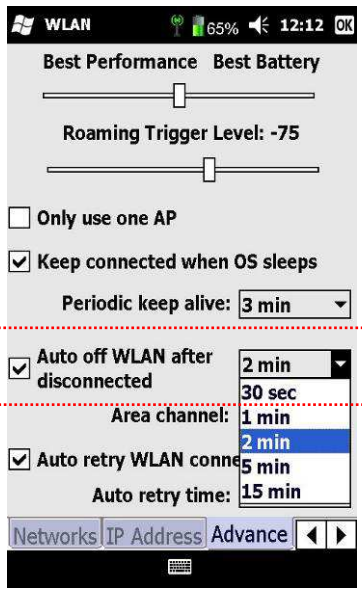
Since PDA is not being notified of such session drop events, new outgoing network traffic from PDA application will suddenly trigger reconnection of Wi-Fi. It means users will experience 10+ seconds delay until connection is re-established.

To avoid connection session drop due to prolonged idle, the PDA has a "Periodic keep alive" feature that would talk to AP periodically to avoid connection session drop. By default, 3-minutes is an optimal value for most APs.

Note:

If idle connection setting could be configured by AP (however, most has no such option), it should be defined such that it is longer than the value of periodic keep alive.

7.9 Wi-Fi Auto off and Auto Connection Retry

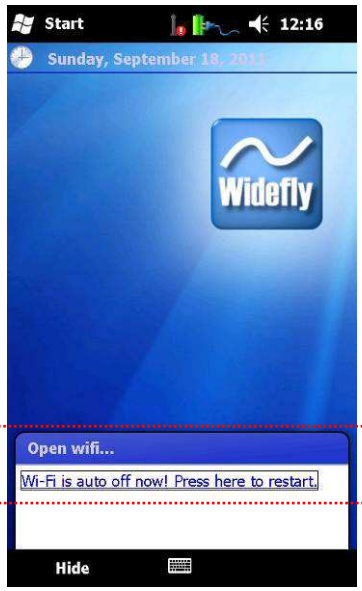


Wi-Fi Auto off

When PDA is out of signal range, system will start searching for SSID in a limited time frame defined in "Auto Off WLAN after disconnected". It is a design to prevent battery from being drained quickly as Wi-Fi searching is a power consuming process. By default, this feature is enabled and WLAN will be off if no AP is found for 2 minute.

Wi-Fi Auto Connection Retry after Auto Off

When Wi-Fi is in auto off state, "Auto retry WLAN connection" will retry connecting to AP if it has been idle for a time frame equal to the value defined in "Auto retry time". If the value is 30 seconds, the feature will wait for 30 seconds before it starts searching for SSID again.



PDA in Wi-Fi auto off state

Thus, if there is no signal, PDA will search AP for 2 minutes and then jump to Wi-Fi auto off for 30 seconds. This cycle will repeat itself until Wi-Fi connection could be successfully established. This process strike a balance between power saving and Wi-Fi connectivity.

Wi-Fi auto off dialog box

When PDA is in Wi-Fi auto off state, a dialog box "WLAN is auto off! Tap here to restart" will be displayed at lower right of the screen. User may trigger reconnection to AP immediately by tapping this without waiting or tapping the Wi-Fi tray icon.

7.10 Notes to Application Developers

When it comes to online POS application, TCP/IP network programming is a key concern to developers because it is the core communication module governing the robustness and stability of the application.

In general, for a PDA online application, its TCP/IP network traffic is either initiated by PDA client or POS server. Different programming approaches should be considered in different scenarios. The following are useful tips for developers concerning about this.

Client-initiated design

- "Wi-Fi always online" feature keeps Wi-Fi connection to the AP even the PDA is in sleep mode. Whenever user presses the power key to wake up the PDA, the client application could immediately send traffic to the POS server without experience any delay.
- Due to the fact the server is always listening to incoming traffics, it is optional for the client application to validate the TCP connection before doing a client-server operation. However, the server initiated traffics are treated differently. Please see the next section for details.

Server-initiated design

- The "Wi-Fi always online" feature allows "server initiated" network traffic even when PDA has entered sleep mode. This allows server to wake up the PDA for alert function or data synchronization request.
- In theory, when PDA has entered sleep mode, any incoming unicast IP package can wake up the PDA from sleeping. However, in practice, the effect depends on the types of traffic sending to the PDA.
- If the sender traffic is a ping request and a connectionless UDP package, it is quite common that a single traffic is not sufficient to wake up the host PDA. More often, it takes several pings or UPD packets to fully wake up the PDA.
- If sender traffic is a connection oriented TCP package, sender's network layer may need auto-retry mechanism until the PDA wakes and acknowledges.
- For the best practices of server initiated traffics, server needs to keep sending alive requests to PDA in every second until the PDA acknowledge before the actual server-client operation.

Chapter 8: Bluetooth

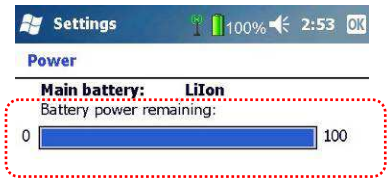
8.1 Overall

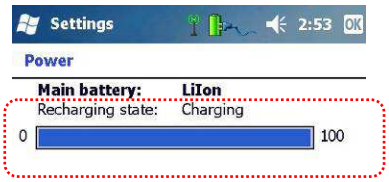
(The content to be completed later)

Chapter 9: Power Management

9.1 Battery & Charging Status

Open Power settings at **Start > Settings > Power**



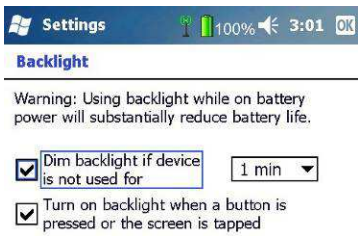


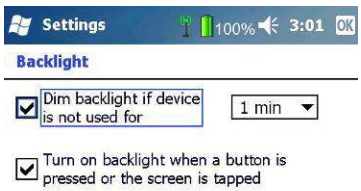
- Running with battery

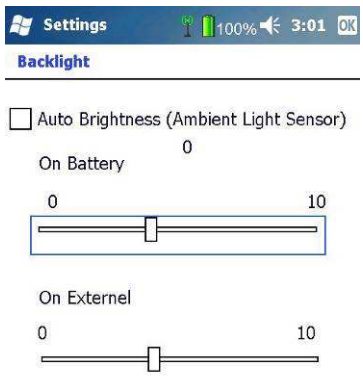
- Battery charging
-

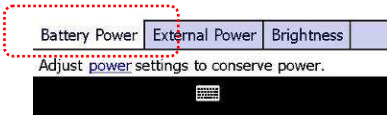
9.2 Dim Backlight Settings

To configure dim backlight settings when the system has been idle for some time, goto **Start > Settings > Backlight.**

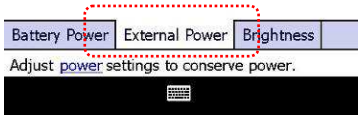

Settings
100%
3:01
OK
Backlight
Warning: Using backlight while on battery power will substantially reduce battery life.
Dim backlight if device is not used for
1 min
Turn on backlight when a button is pressed or the screen is tapped



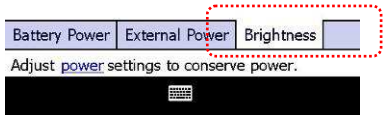




"Battery Power" page



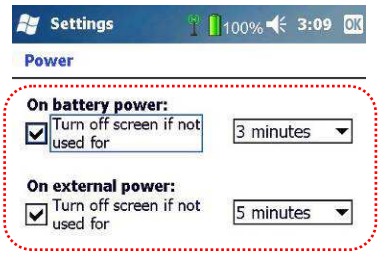
"External Power" page

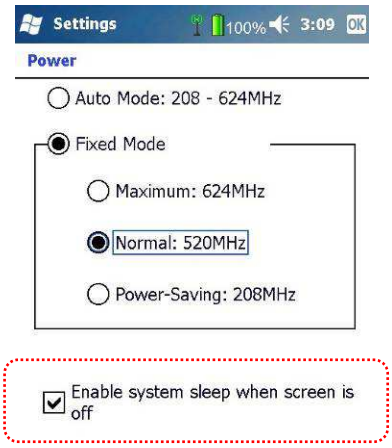


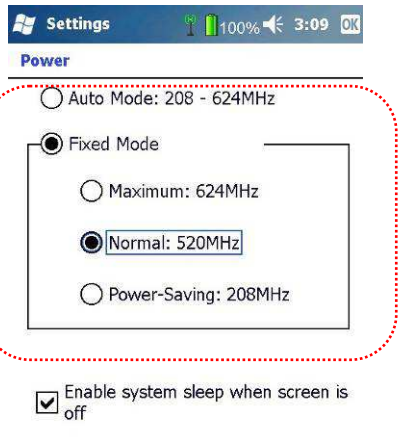
"Brightness" page.

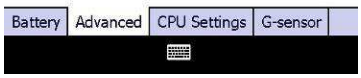
9.3 Turn off Screen/LCD, System Sleep & CPU Speed

To configure screen/LCD turn off settings when the system has been idle for some time, goto **Start > Settings > Power > Advance (page).**









By default, screen/LCD is turned off after 3 minutes idle

This options enabes "System Sleep" when screen/LCD is off.

Default CPU speed is 520MHz.

9.4 Sleep Mode Explained

System Sleep Mode

"Sleep Mode" is a unique power saving feature innovated by Widefly. This mode enables exceptionally low power consumption like power off status while the Wi-Fi connection could still be kept. This mode empowers "Always-on Wi-Fi" even the system is in deep sleep status.

To enter "Sleep Mode" when the screen is turned ON:

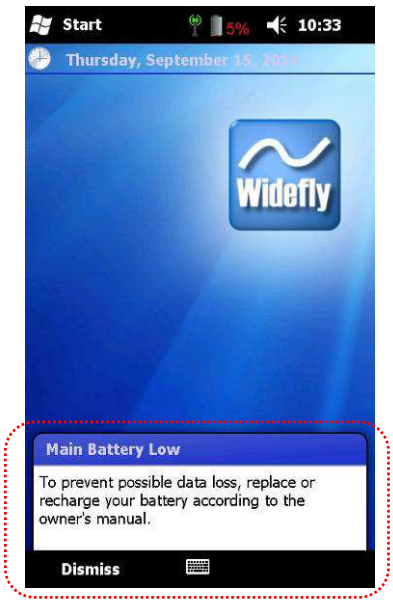
- Press power key or
- Put the PDA upside down for 5 seconds. This will enable auto screen off (This also requires option "Enable system sleep when screen is off" selected)

System Wakeup

When PDA is in "Sleep Mode", it could be woken up by:

- Pressing the power key. This also turns ON the screen & backlight. OR
- Incoming network traffic (TCP/IP/ICMP network packets).
  For example, POS server program may send data to PDA client programs while they are sleeping. Once system is reverted to normal, client programs are able to process the data from POS server. Another example is PDA being pinged by the external networks. Note that this kind of wakeup will NOT turn on screen & backlight.

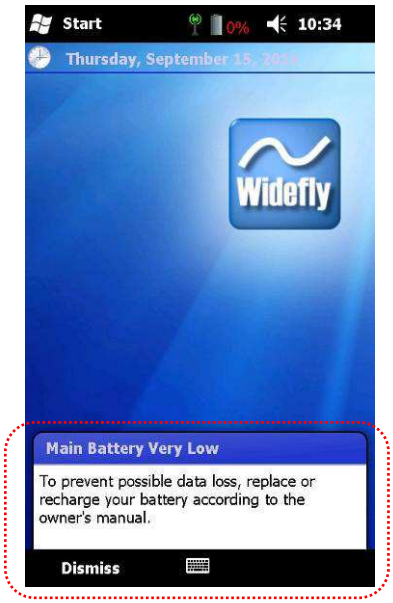
9.5 Battery Low



Battery Low Warning – 5%

When battery level drops to 5%

- Power indicator / LED turns to red Flash
- "Main Battery Low" notification will be popped up.



Battery Very Low Warning – 0%

When battery level drops to 0%

- Power indicator / LED remains in red solid
- System will be shutdown automatically

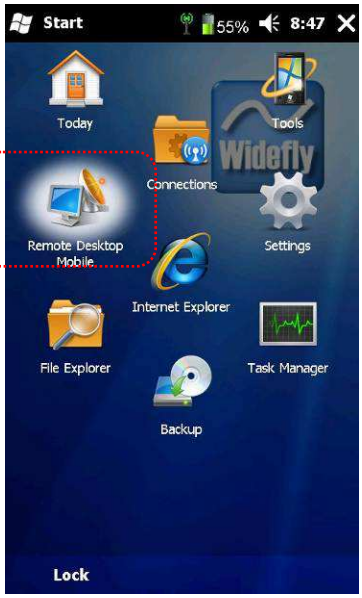
Note:

- If battery level is too low, it may not be able to boot up the system and NO LED light is showed when power key is pressed. In that case, recharge of battery for 10-15 minutes is required to recover the battery level.
- For normal battery power, pressing power key will either show green or red LED. Red indicates insufficient power to boot up the operating system.
- User is advised to recharge the empty battery or battery lifetime will be shortened if such empty state has been stayed for a long time.

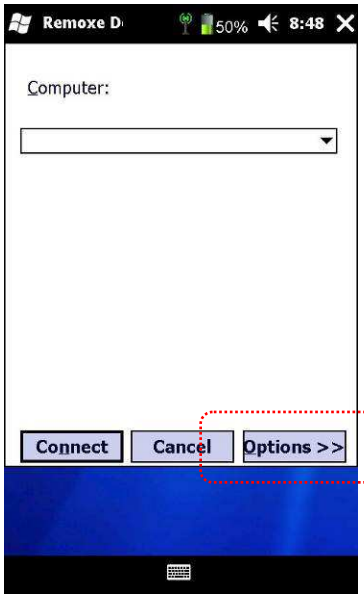
Chapter 10: Terminal Services Client / Remote Desktop

10.1 Create TSC/RDP Profile

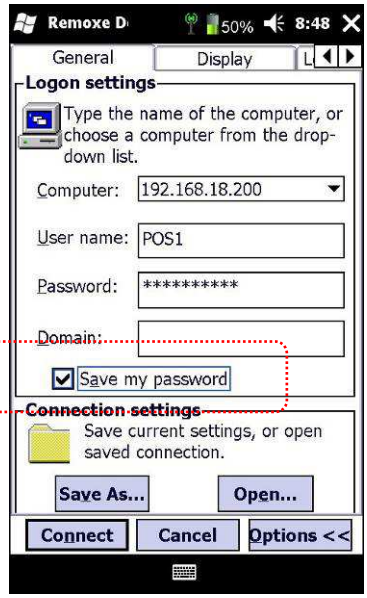
Different from other Windows Mobile PDAs, WF43 uniquely supports Microsoft Terminal Services Client (TSC) / Remote Desktop (RDP) with auto-login, auto-start application as well as COM port redirection feature. Note: TSC & RDP are the same terminology used by Microsoft. To create a RDP profile, follow the screens below.



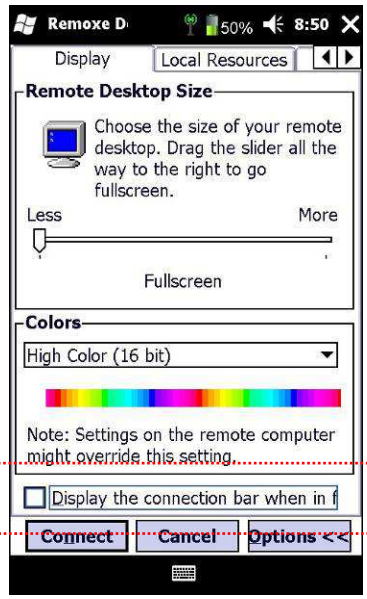
- Goto **Start > Remote Desktop Mobile**



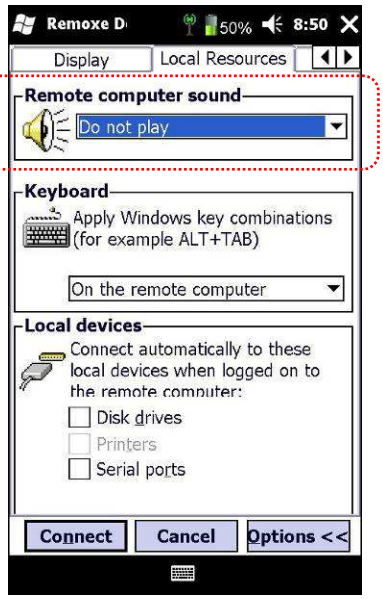
- Tap "Options" to expand detail setup fields



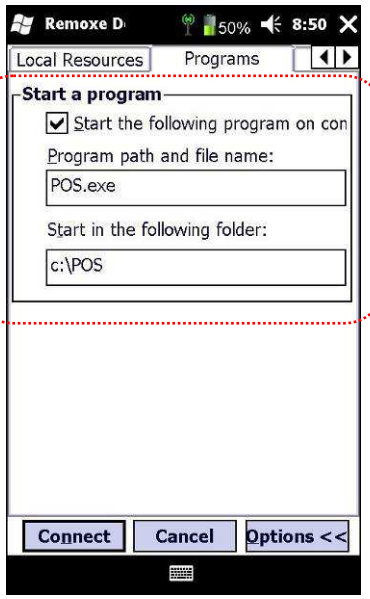
- Enter all info especially the logon username & password
- Select "Save Password"



- Uncheck to hide connection bar at the RDP screen top

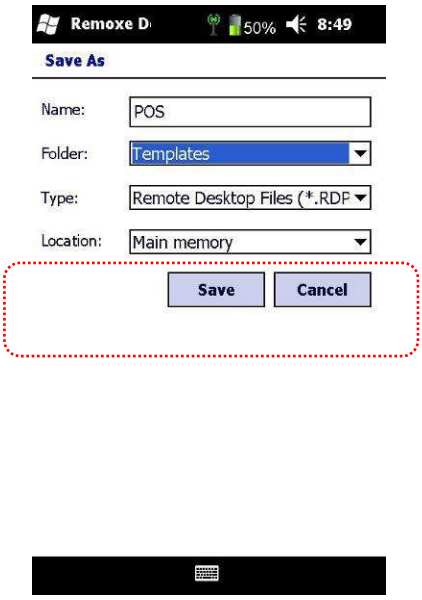


- Disable remote sound from being played on PDA



- Configure auto run program and its startup folder. Leaving blank will start

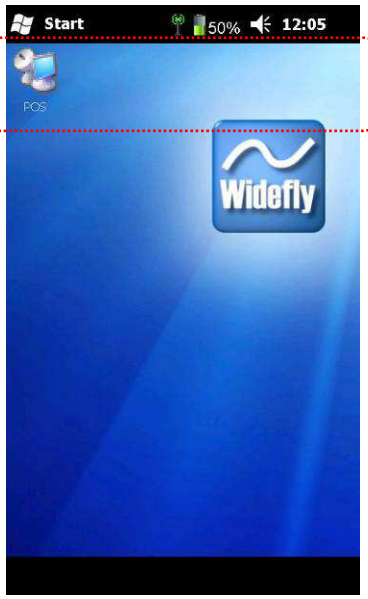
standard Windows desktop.



- Go back to page "General" and press "Save As" (Remember to check "Save my password" option).

- Open file explorer and check if the RDP profile file exists
- Tap the RDP file to run RDP session

- RDP session established. Note that SIP (Soft Input Panel) is shown at the bottom screen.



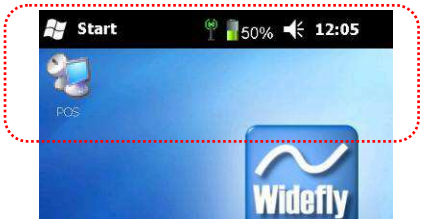
- If RDP profile shortcut is placed on today screen, bottom SIP will be hidden. See next screen capture.
- For details, please refer to the next section 10.2

- Bottom SIP is hidden (if RDP session is started via Today Screen).

10.2 Create RDP shortcut at Today Screen

It is most intuitive to start a RDP session if end-users could directly run it via Today Screen.

For the detail steps creating RDP shortcut on Today Screen, please refer to Chapter 16 – Configuring Today Screen. Below are some screen shots placing the RDP shortcut of today screen.



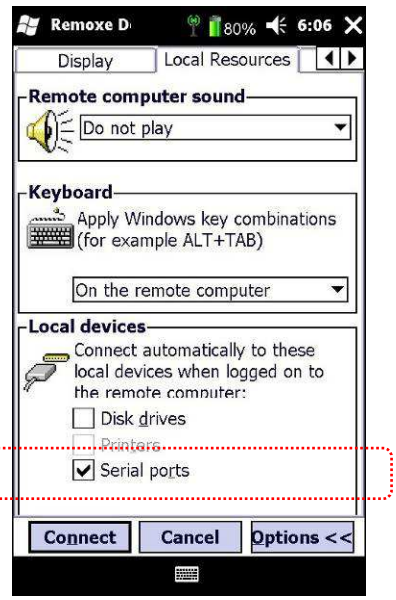
- Place a RDP shortcut at today screen

- Place a ToggleStart utility to show/hide top taskbar

- Tap taskbar is hidden

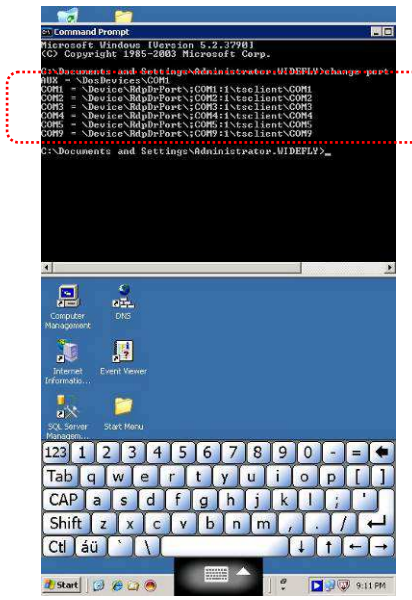
10.3 Serial Port (COM Port) Redirection

COM port redirection is a very important feature if RDP application requires communicating with PDA's local COM port, i.e. accessing local port remotely from the server. Typically use is to open barcode scanning COM port for getting scanning result or to open Bluetooth generated virtual COM port to print receipts. To create a RDP profile with COM port redirection enabled, follow the steps below:



- At page "Local Resources", enable "Serial Ports". Save the settings into profile file.

- For the first time RDP is run, it pops up a warning message serial ports are being redirected to RDP server.
- Select "Don't prompt me again…" to disable this warning.



- Run cmd.exe and type "Change port /query". This will list all ports including server's local ports and PDA's redirected ports.
- For example, COM9 is the redirected port for barcode scanning result.

10.4 Magstripe Card Reader (MSR)

Unlike previous model WF35, WF43 does not require to have special RDP configuration when MSR is used. (WF35 needs to modify KeyboardHookMode setting).

10.5 RDP Profile File Format

RDP profile file is indeed an UNICODE text file. Advanced RDP settings could be configured by modifying the file content. To open the file for edit purpose, goto **Start > Tools > lgtEditor**. Note that lgtEditor is a freeware. For details, please refer to Chapter 17.

RDP profile file could be edited to change its behavior. The table below is technical reference of the RDP profile file format.

Keyword:type:value	Description
AudioRedirectionMode:i:0	Indicates where the audio plays. A value of zero (0) indicates that the audio plays on the host computer. A value of 1 indicates that the audio plays on the remote device. A value of 2 indicates that the audio does not play.
AutoReconnectionEnabled:i:1	Indicates whether an attempt is made to automatically reconnect to the host if a connection is lost. A value of 1 indicates that automatic reconnection is enabled. A value of zero (0) indicates that it is disabled.
BBarEnabled:i:1	Indicates whether to display the connection bar. A value of zero (0) indicates that the connection bar is not displayed. A value of 1 indicates that it is displayed.
BBarShowMinimizeBtn:i:1	Indicates whether to display the minimize button on the connection bar. A value of zero (0) indicates that the minimize button is not displayed. A value of 1 indicates that it is displayed.
BbarShowPinButton:i:0	Indicates whether the pin button on the connection bar is displayed. A value of zero (0) indicates that pin button is not displayed, the connection bar remains on top, and all server output will appear below it. A value of 1 indicates that the pin button is displayed so that a user can unpin the connection bar from the UI.
BBarShowRestoreBtn:i:1	Indicates whether to display the restore button on the connection bar. A value of zero (0) indicates that the restore button is not displayed. A value of 1 indicates that it is displayed.
BBarPinned:i:1	Indicates whether to pin the connection bar to the shell. A value of zero (0) indicates that the connection bar is hidden automatically when the cursor is moved away from the connection bar. A value of 1 indicates that the connection bar is always displayed.
BitmapCacheSize:i:1500	Specifies the size, in KB, of the bitmap cache in memory. The maximum value is 32000.
BitmapPersistCacheLocation:s:\Temp	Indicates the location of the bitmap cache.
BitmapPersistenceEnabled:i:0	Indicates whether bitmap caching is selected. A value of zero (0) indicates that bitmap caching is not selected. A value of 1 indicates that it is selected.

ColorDepthID:i:4	Indicates the color depth in bits per pixel (bpp). A value of zero (0) indicates 4 bpp. A value of 1 indicates 8 bpp. A value of 2 indicates 15 bpp. A value of 3 indicates 16 bpp. A value of 4 indicates 24 bpp. The default value is either 24bpp, or the color depth at which the OS boots, whichever is less.
Compress:i:1	Enables file and directory compression. Compression is on by default and it is recommended that it remain so.
ConnectToServerConsole:i:0	Used only in non-Windows-based Thin Client configurations. It indicates the console to connect to from the command line. A value of zero (0) indicates that the command connects to a Terminal Services session. Windows XP Professional ignores this setting. A value of 1 indicates that the command connects to the host console.
desktopheight:i:1024	Indicates height of the display, in pixels. The default value is the resolution at which the OS boots.
desktopwidth:i:1280	Indicates width of the display, in pixels. The default value is the resolution at which the OS boots.
disable full window drag:i:1	Indicates whether full window drag capability is enabled or disabled. A value of 1 indicates that full window drag is enabled. A value of zero (0) indicates that it is disabled.
disable menu anims:i:1	Indicates whether menu animation is enabled or disabled. A value of 1 indicates that animation is enabled. A value of zero (0) indicates that it is disabled.
disable themes:i:0	Indicates whether themes are enabled or disabled. A value of 1 indicates that themes are enabled. A value of zero (0) indicates that themes are disabled.
disable wallpaper:i:1	Indicates whether wallpaper is disabled or enabled. A value of 1 indicates that wallpaper is enabled. A value of zero (0) indicates that it is disabled.
DisableFileAccess:i:1	Indicates whether the user has access to the local file system. A value of 1 indicates that access to the local file system is disabled and the **Save As** and **Open** buttons are not available in the UI. A value of zero (0) indicates that the user has access to the local file system.
domain:s:C1554501-A	Indicates the domain of the person who can log on to the remote device. There is no default.
EnableDriveRedirection:i:1	Indicates whether drive redirection is enabled. A value of 1 indicates that drive redirection is on. A value of zero (0) indicates that it is off.
EnablePortRedirection:i:1	Indicates whether COM port redirection is enabled. A value of 1 indicates that COM port redirection is on. A value of zero (0) indicates that it is off.
EnablePrinterRedirection:i:1	Indicates whether printer redirection is enabled. A value of 1 indicates that printer redirection is on, and a value of zero (0) indicates that it is off.
EnableSCardRedirection:i:1	Specifies whether redirection of smart cards is allowed. A value of 1 indicates that redirection of smart cards is on. A value of zero (0) indicates that it is off.
KeyboardHookMode:i:2	Indicates what is displayed when ALT-TAB is pressed on the

	keyboard. A value of zero (0) indicates items on the local device are displayed. A value of 1 indicates items on the remote device are displayed. A value of 2 indicates that the device is full-screen only.
MaxReconnectAttempts:i:20	Indicates the maximum number of attempts that are made to reconnect to the host after a connection is lost.
MCSPort:i:3389	Indicates the alternate Winsock port for the RDP. The default value is 3389. Change this value to an appropriate value if the terminal server is listening on a different port.
Password:s:<*password*>	Indicates the password of the person identified in the UserName keyword. **Note** Windows CE reads saved passwords, but does not have the ACLs to securely write passwords.
ServerName:s:65.4.18.	Specifies the IP address of the remote device.
StartFullScreen:i:1	Indicates whether the Terminal Service session starts in full screen. A value of 1 indicates that the session starts in full screen. A value of zero (0) indicates that it does not.
AlternateShell:s:<*startup shell or application*>	Indicates the alternate shell or startup application to use in a session. **Note** You can restrict usage after a user logs in by setting this value to a specific application on the server. The user will only be allowed to use the application that you specify.
UserName:s:<*name*>	Indicates the user name of a person who can log on to the remote device.
WorkingDir:s:<*folder*>	Indicates the folder that contains the alternate shell or startup application.

10.6 Common modifications of RDP profile file

The following are common modifications of RDP profile file

Keyword:type:value	**Common modifications**
BBarEnabled:i:1	Default: 1 (show top connection bar) Modification: 0 (to hide the bar)
AlternateShell:s:<*startup shell or application*>	Default: <empty> Modification: <designated POS app, e.g. c:\POS\POS.exe>
WorkingDir:s:<*folder*>	Default: <empty> Modification: <working folder of the POS folder, e.g. c:\POS\>
Password:b:<password>	Default: <empty> Modification: <encrypted password generated by "Remote Desktop Mobile" shortcut>
UserName:s:<name>	Default: <empty> Modification: <username filled by "Remote Desktop connection" shortcut>
ServerName:s:<RDP server>	Default: <empty> Modification: <IP address filled by "Remote Desktop connection"

	shortcut>
Disable Themes:i<flag>	Default: <0> Modification: <1> This will disable Windows theme to accelerate screen performance
EnablePortRedirection:i:<flag>	Default: <0> This will not enable serial port redirection Modification: <1> This will EnablePortRedirection:i:1
AudioRedirectonMode:i<flag>	Default: <0> This will redirect server audio to PDA client Modification: <2> This will disable sound playing on RDP client & server

10.7 Best Practice deploying RDP Application

The following are important tips to deploy a RDP solution.

Best Practice	**Reason**
Assign username per PDA unit (e.g. PDA01, PDA02, PDA03)	▪ Administrator could identity a RDP session and its associated processes (application) by username ▪ In case of issue, administrator could end the session or kill the process for a specific PDA unit
Disable screen saver	▪ For each username running RDP application (e.g. PDA01, PDA02), screen saver **MUST** be disabled Note: screen saving setting is user specific ▪ RDP client displays whatever remote desktop is displaying. When the desktop is screen saving, a complete black screen is displayed in the PDA screen. ▪ Users may think that PDA is in sleep mode. However, pressing power key will not wake up but to bring PDA into sleep mode, also a black screen. After several power key attempt, users may consider there is an issue in PDA or application
Restrict each username to one session	▪ In "Terminal Services Configuration" > Server Settings, define "Yes" to "Restrict each user to one session" ▪ This avoids repeated logon exceeding the license count
End users access to RDP profile under user mode only	▪ Avoids accidental changes of RDP profile file content that causes problem in connecting to RDP server

Screen saver MUST be disabled for the username used for RDP application.

Chapter 11: System Clone / Backup / Restore

11.1 Introduction

WF43 is a unique POS PDA features powerful System Clone (similar to PC Norton Ghost utility*), Backup / Restore & ROM upgrade tools at no additional cost. Since this is a feature fully integrated with the system ROM, it is always ready to use for a brand new unit or an unit after clean reset (restored to factory default settings).

With backup tool and user mode locking PDA configurations, it dramatically changes the way of deploying & supporting PDA solutions. To see the benefits, see the comparison below:

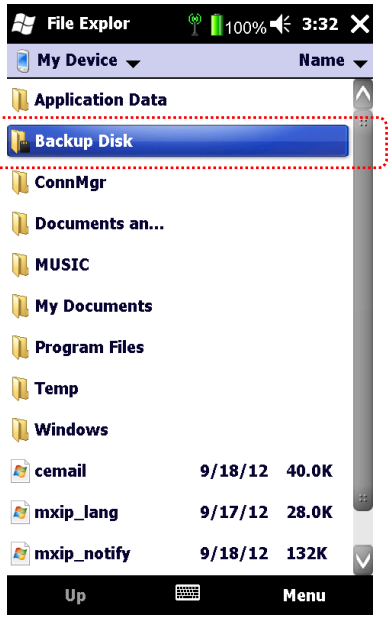
Scenario	Consumer PDA	Widefly PDA
PDA Setup	▪ Setup one-by-one, very time consuming ▪ Must be performed onsite ▪ Standardization of configurations is very difficult	▪ Prepare one master image and clone to many PDAs ▪ All backup images could be prepared at office before restoring to PDA onsite
Local Backup Disk	▪ No local backup disk ▪ Extra SD Card is required for each PDA and is subject to loss easily	▪ Default 40MB backup disk is created locally on the PDA ▪ Individual system backup could be stored in this local backup disk ▪ No extra SD Card is required
Accidental changes of PDA setup	▪ Very easily ▪ Create interruption to operations ▪ Onsite support required	▪ Virtually zero support as end users cannot change any configurations in User Mode
Performance of restore	▪ Slow ▪ Typically more than 5 minutes	▪ Very Fast ▪ Typically less than 2 minute
ROM upgrade	▪ Separated utility and procedure ▪ Need PC & USB cable ▪ Upgrade one-by-one	▪ A SD card is sufficient to upgrade ▪ Upgrade many units at the same time as long as there are many SD Cards
Cost	▪ License cost per PDA unit	▪ Come with free of charge

* Note:
Norton Ghost is a product of Symantec. Symantec is a registered trademark of Symantec Corporation. (http://www.symantec.com)
This tool is available for ROM v1.0.28 or above.

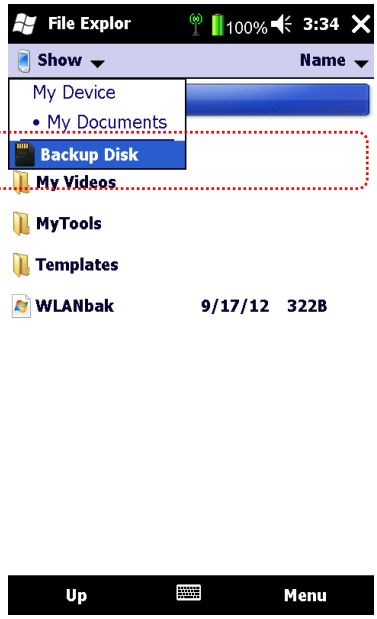
11.2 Local Backup Disk

A 40MB local backup disk is partitioned from the onboard flash memory.

This local backup disk is specially designed not to erase any files in local backup size if Clean Reset is performed. This is to ensure system administrators or end users still have the chance to retrieve the last known good backup image.



- At root directory "My Device", folder "Backup Disk" refers to partitioned local backup storage.



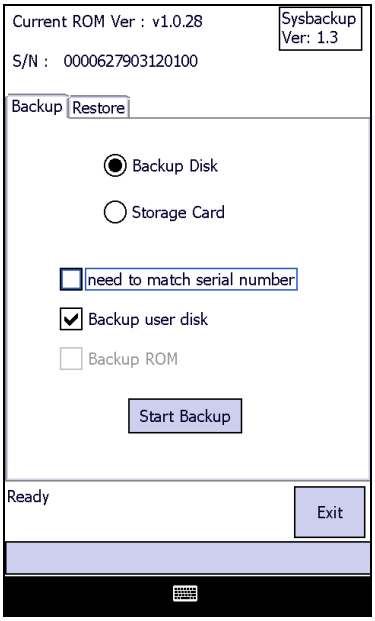
- "Backup Disk" is like SD card, this can be direct accessed via top right "Show" button of the file explorer

For the best practice of PDA deployment, system administrators should create a snapshot backup image and store it locally for each PDA every time when there are configuration changes.

In case of system recovery, end users could restore from this local backup image quickly and effortlessly without calling the technical support. This helps realize zero support of the PDA and significantly cut support cost. To end users, this self-service recovery would minimize interruption to PDA operations.

11.3 System Clone / Backup

Under Admin mode, **Goto Start > Backup**.



System Backup

Select the first main tab page "Backup". To perform backup, follow the steps below:

- Select either "Backup Disk" or "Storage Card". Storage card refers to external SD card.
- Need to match serial no: If checked, backup image could only be restored on the same PDA
- Backup user disk: This is the default and recommended backup option as it enables fast system restoration by creating small backup image, typically in few MB.
  This option is best used with "\Backup disk" location. However, it also requires restore on the same ROM version.
- Backup ROM: This creates backup image with ROM files, typically more than 80MB and requires the SD card as backup destination. This option is best used for ROM upgrade purpose.

Note:

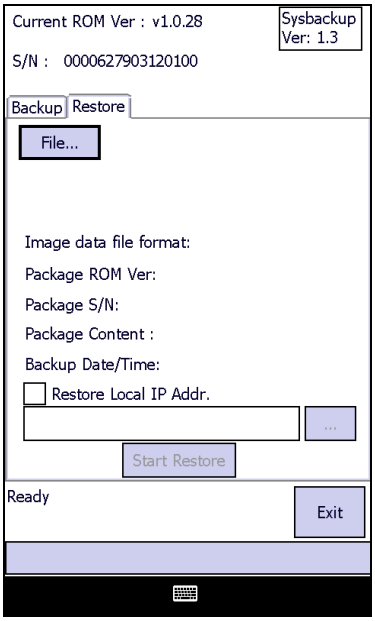
- Backup option is disabled in user mode but restore is allowed.
- Backup filename is in format backupCCYYMMDDHHMMSS.img
- Backup would not start if battery is under 50%. However, this checking doesn't apply if PDA is being charged
- When backup finishes, it must be rebooted.
- Although backup function creates exact copy of image of the complete system, some settings may not work after the image is restored to the unit different form the original one.
  One example is the RDP profile file. The file contains encrypted logon password that is encrypted by device's unique MAC address. Thus, restored unit with encrypted password is no longer valid.

Backup creates exact copy of complete system. However, some functions may not work as expected on restored unit.

For example, since RDP profile file contains encrypted saved password by the original unit's MAC address, restored unit may find the password invalid. To rectify it, the profile file has to be re-opened with correct password and save again.

11.4 System Restore

Under Admin mode, **Goto Start > Backup**.

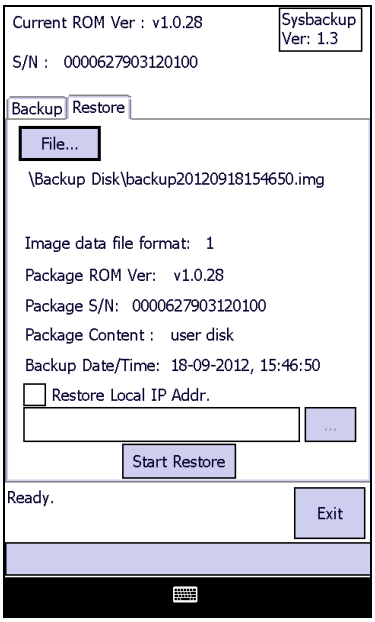


System Restore

There are 2 types of backup image (also called package). "User Disk" or "ROM + User Disk".

"User Disk" refers all system settings and installed components and programs excluding system ROM. The file size is typically very small in few MB. It is because "User Disk" is a smart format that contains only changes of the system.

"ROM + User Disk" is same as the "User Disk" type except it also contains the ROM files. Thus, its typical size is bigger than 80MB.



Step 1: **Precaution for ROM upgrade!!!**

- If the backup image contains ROM file, it is HIGHLY recommended PDA is plugged with the charger.
- Should power suddenly stop during restoring, ROM files may be corrupted, which means returning to factory for repair may be necessary

Step 2: Select backup image

- Press "File" and select a backup image. The image can be from local backup disk or storage card.
- The image (package) detail info is displayed. For example, package ROM version, S/N, last backup date/time and etc.
- To override SSID and IP info from the original backup image, a WLAN profile INI file could be selected. For details, please refer to next section "System Restore with WLAN profile Override"

Step 3: Select Restore

- Press "Start Restore" to proceed restore function.
- If the package contains ROM files, it takes longer to complete the restore.

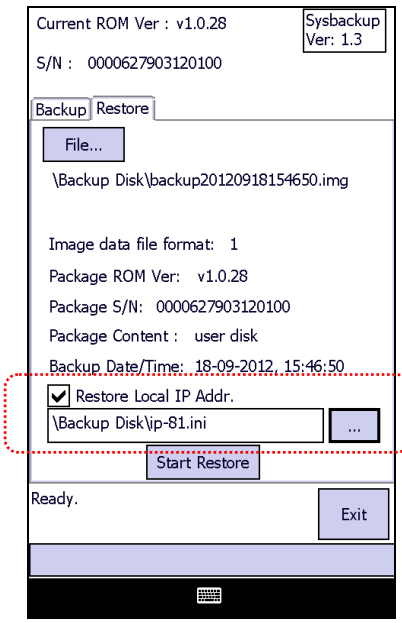
Note:

- Restore is allowed on both admin & user mode
- Restore would not start if battery is under 50%. However, it doesn't apply if PDA is being charged
- After successfully restore and press OK, PDA will be rebooted.

11.5 System Restore with WLAN profile Override

Apart from the convenience that system administrators could deploy many PDAs by restoring a master copy of PDA clone image, different WLAN profiles including SSID, authentication, encryption, IP address, DNS address & etc, could also be applied per restore task.

This is a very handy feature that not only enables standardization of application settings, it also allows restoration of the specific IP and WLAN info when PDAs are being deployed to the production environment, which SSID & IP address are different from the master copy of PDA image.



Restore with WLAN profile override

Under restore tab page, select the option "Restore local IP Addr", tap the "…" button to select an INI file. This file contains SSID and IP info.

The INI format is described in the next paragraph.

File format – WLAN.ini

The following is a WLAN.ini file that could be used for restoring specific WLAN & IP address info.

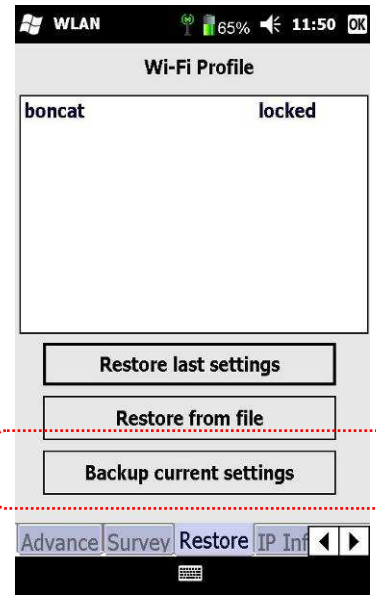
```
DHCP=0                          ← 0: Fixed IP / 1:DHCP
IP Address=192.168.18.51        ← For fixed IP, the assigned IP address
Subnet Mask=255.255.255.0       ← For fixed IP, the subnet mask
Default Gateway=192.168.18.1    ← For fixed IP, the default gateway
Primary DNS=192.168.18.1        ← For fixed IP, the primary DNS
Second DNS=                     ← For fixed IP, the secondary DNS
Primary WINS=                   ← For fixed IP, the primary WINS
Second WINS=                    ← For fixed IP, the secondary WINS

SSID=WFWEP              ← SSID of the Wi-Fi network
NetworkType=1           ← 1: AP mode
SecurityType=1          ← 0: Open / 1:Shared / 4: WPA-PSK / 7: WPA2-PSK
EncryptionType=1        ← 0: WEP / 4: TKIP / 6: AES
Networkkey=1234567890   ← clear text network key **
NetworkkeyBin=          ← encrypted network key generated by the WLAN panel
WEPKeyIndex=1           ← WEP key index.  Most often is 1
SingleNetwork=1         ← 1: single SSID
```

** **Note:** clear text network always overrides binary encrypted network key

WLAN.ini from Wi-Fi Panel

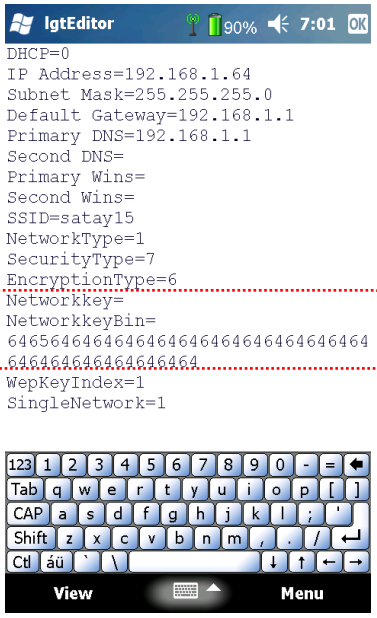
To get the current WLAN and IP info as INI file, open WLAN panel (**Start > Settings > Wi-Fi, "Restore" tab page**).



Backup WLAN / IP current settings

Under restore tab, press "Backup current settings" and save the INI file onto the backup or storage card.

This INI file could also be used for restoring the WLAN profile and IP info.



To edit the file, use text editor to open it (**Start > Tools > IgtEditor)**.

The file could be edited and deployed to customer sites with pre-defined SSID & IP info.

Note:

- The value of "NetworkkeyBin" is encrypted network key generated by the WLAN backup function. This is by designed not readable for security purpose.
- Clear text network key could be placed on the "Networkkey". If this clear text key is intentionally used for deployment purpose, it always overrides the encrypted key. This facilitates manual input of network key in the INI file.

Chapter 12: Magstripe Card Reader (MSR)

12.1 Introduction

The Magstripe Card Reader USB add-on module (WF43MSR) is designed from scratch for reliability, security, durability, affordability & software compatibility.

Unlike common CF/SD card based MSR solutions, WideFly's MSR has a far more reliable attachment mechanism which could withstand heavy duty and frequent swiping of credit cards / magstripe cards in busy hospitality environment.

WF43 w/ WF43MSR

For data security, the MSR has a unique encryption feature at MSR's hardware level. The encryption key can be configured by POS ISVs/SIs. This reduces the risk customer credit card data, originally presented in clear-text format, could be captured by unauthorized persons or trusted programs (e.g. notepad).

Since customers have no idea what program is actually running on the PDA, it simply cannot tell whether their cards data are processed securely within a trusted POS application or is stolen for mis-use. The encryption feature avoids potential mis-use of credit card data because only trusted POS applications, integrated with WideFly decryption SDK/API, could decrypt the card data within the application memory.

WideFly's MSR design is programming friendly. Since MSR emulates keyboard input, integrating with POS application is as easy as reading a text field. It doesn't require special programming interfaces like ActiveX, DLL & RS232. This also allows easy RDP application development.

12.2 Attaching WF43MSR to PDA

- MSR front view

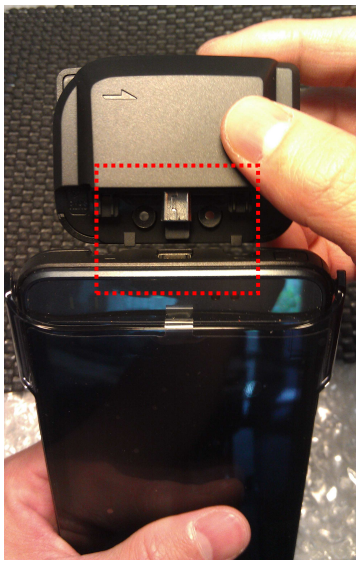
- Rear view (S/N label)

- Bottom view (USB client)

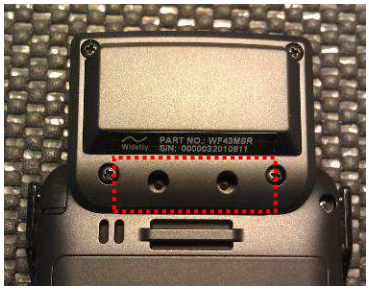
- PDA rear top is the USB host cover.

- To open it, remove the pair of screws

- USB host cover removed



- Insert MSR's USB plug to the USB host socket located at PDA top



- MSR is firmly held at the PDA top
- Screws should be applied to strengthen the attachment

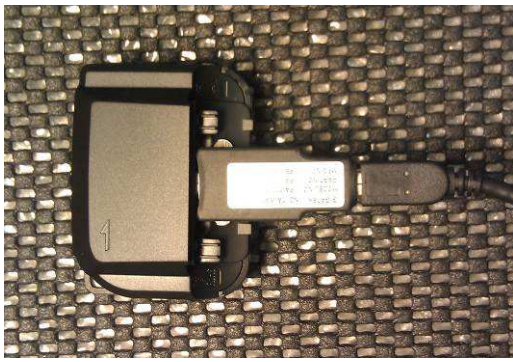
- Status bar shows MSR icon if MSR is inserted to the USB host

12.3 Configure MSR by Configuration Utility

The utility could be downloaded from Widefly FTP server. For details, please refer to Chapter 17 – FTP download

- USB converter board for WF43MSR

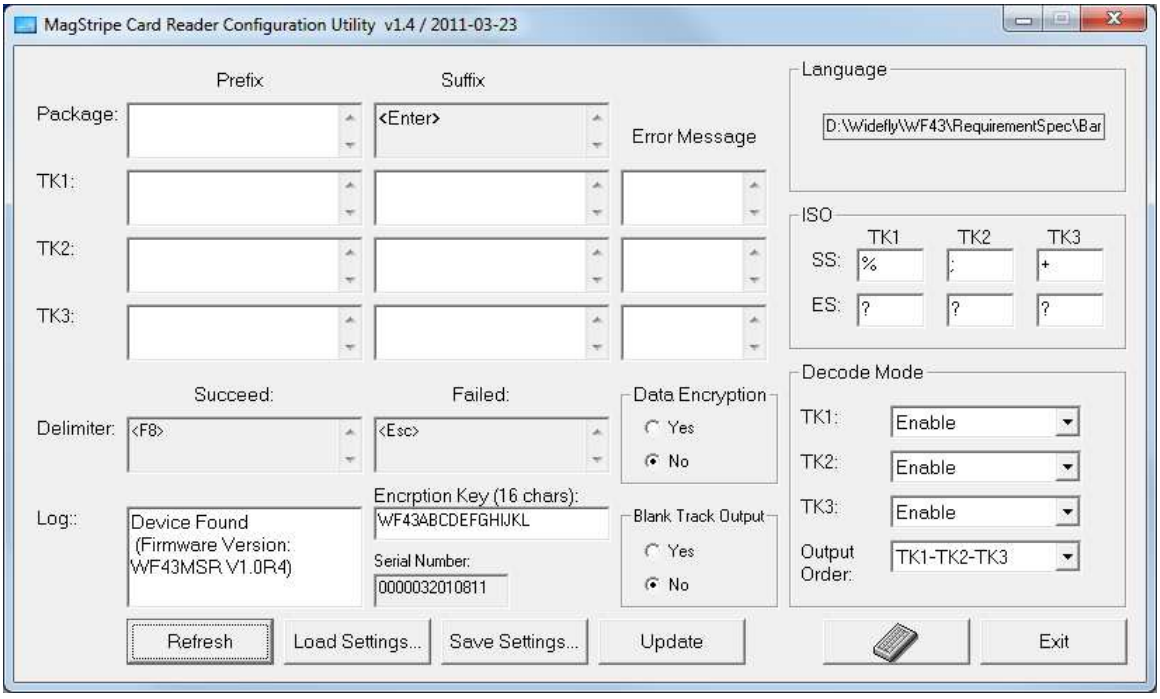
- Mini-USB cable connected with the converter



- WF43MSR connected with the USB cable + converter

To configure the MSR, connect another end of USB cable to PC (Windows XP/Vista/7). The device is specially designed that it could auto detected by the operating system.

The settings of WF43MSR could be modified by a Magstripe Card Reader Configuration Utility running on PC. Run the configuration utility "hid_msr.exe".



Configuration	Notes
Package Prefix / Suffix	Additional Prefix / suffix characters can be added to beginning / ending of 3-track data For example, it is very common to add newline at package suffix. So, newline is the default suffix.
TK[1/2/3] Prefix / Suffix	Additional prefix / suffix can be added to track 1/2/3
TK[1/2/3] Error	If there is error reading a track, specific error message could be

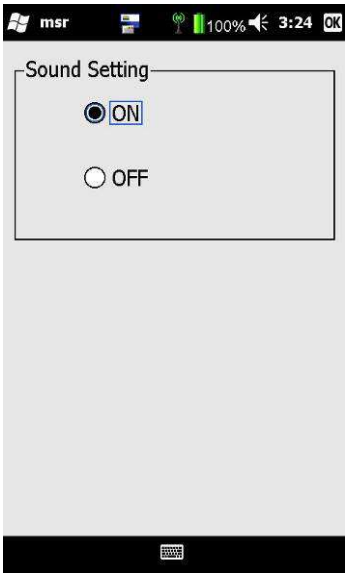
Configuration	Notes
Message	defined. By default, it is empty. For example, you may define "ERR" as error message
ISO TK[1/2/3] SS/ES	SS is start sentinel / ES is end sentinel According to ISO standard of magstripe card data: Track1 SS/ES: % / ? Track2 SS/ES: ; / ? Track3 SS/ES: + / ?
Decode Mode	Some tracks may be disabled Default track data order is TK1-TK2-TK3
Data Encryption	Yes or No. By default, data encryption is No.
Encryption Key	A 16-characters key. By default, the key is "WF43ABCDEFGHIJKL" It is recommended to change this key for production environment
Blank track output	If this is YES, empty track will send track prefix/suffix as well as SS/ES with empty data. Default is NO
Serial Number	MSR serial no (S/N). For MSR demo unit, S/N is empty.
Load / Save Settings	Settings can be saved / loaded via a text file.
Refresh	Refresh to re-connect MSR. Note that "refresh" does not retrieve settings from MSR internal memory.
Update	Write all MSR settings to the MSR internal memory
Delimiter	Reserved fields. Read only.

To update configuration of a MSR, follows the steps below:

- Connect mini-USB cable + converter + MSR and plug the USB cable to PC
- Run the configuration utility and input new settings. Note that the utility does NOT retrieve current settings of the MSR but to write new settings to the MSR.

12.4 Configure MSR sound by WF43

Goto **Start > Settings > MSR**



Sound Setting

- Default is ON.

  When MSR is plugged to the PDA, system will play a MSR plug-in sound and the taskbar displays a MSR icon. Similarly, when the MSR is removed, system will play a sound and hide the taskbar MSR icon.

12.5 MSR data encryption

Data encryption is a unique feature to protect clear-text credit card (or Magstripe card) data from being copied easily by notepad or any untrusted applications.

Clear-text data without encryption

- By default MSR encryption is off.
- Card swipe will generate clear-text keyboard input that could be captured by Notepad

Download MSR Decryption Utility

- This decryption utility demonstrates how decryption mechanism could be incorporated to the POS application. Thus, only trusted application could decrypt the card data within program memory

Note: The source code as well as EXE file of this utility could be downloaded from the FTP server. Please refer to Chapter 17 – FTP Download.

12.6 MSR data encryption via RDP

Application running via RDP is indeed server-side application. WideFly MSR works perfectly with server-side RDP POS application as well as local PDA application.

To demonstrate MSR via RDP, follow the screenshots below:

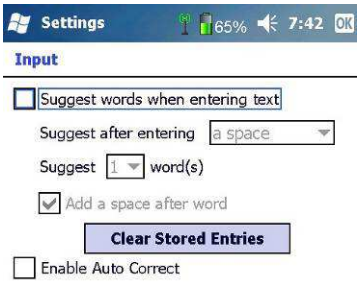
- Establish RDP session from PDA to server
- Run "MsrAesTester.exe" at server side. First, locate focus on "Input a string" box and swipe a credit card at WF35.
- Press "Decrypt" to retrieve original card data

The POS app could integrate with this decryption library (DLL) so that credit card data could be processed securely within application.

Note: The source code as well as EXE file of this utility could be downloaded from the FTP server. Please refer to Chapter 17 – FTP Download.

12.7 Disable Word Completion

Since WF43MSR emulates keyboard input, Windows Mobile "Word Completion" must be disabled and this is the default configuration. Otherwise, MSR input will become slow because of accumulated word completion database.



To disable Word Completion:

- Uncheck "Suggest words when entering text"
- Uncheck "Enable Auto Correct"

If the word completion database has grown too big that it impacts MSR input speed, press "Clear Stored Entries" will clean it up.

Chapter 13: Barcode Scanner

13.1 Introduction

Similar to WF43MSR, Widefly has developed an USB add-on device for Barcode Scanner (WF43BS1). The device is a Laser Class 1 barcode scanner powered by reliable, durable and high performance scanning engine from Motorola.

Unlike common CF/SD card based Barcode Scanning solutions, WideFly's Barcode Scanner has a far more reliable attachment mechanism which could withstand heavy duty and frequent scanner in busy hospitality environment.

The scanner is uniquely designed to accommodate keyboard emulation and serial port input requirements.

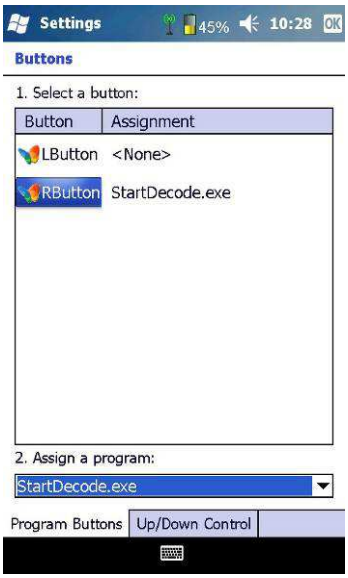
For key emulation, it will be as simple as keyboard input and thus very friendly to developer without additional OCX/DLL and programming facility. This also facilitates simplify data capture in RDP environment.

WF43 w/ Barcode Scanner

If asynchronous data capture is required (i.e. data is collected in background without UI focus), the scanner could be configured to send data via serial port instead of to emulate keyboard inputs.

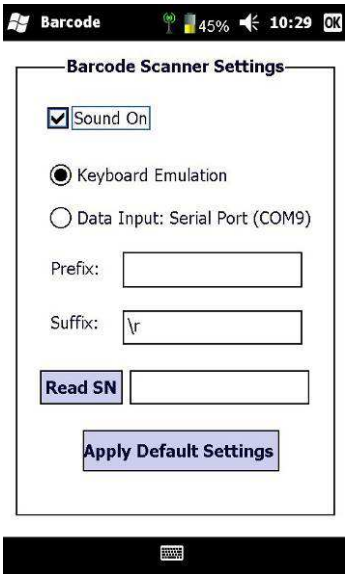
13.2 Configuring Barcode Scanning

Barcode scanning could be triggered by left or right shortcut keys. Goto **Start > Settings > Inputs & Languages > Buttons.**.



Assign scanning program to shortcut key

- Either left or right shortcut could be assigned
- Assign program "StartDecode.exe" to the desired shortcut key.
- Press OK



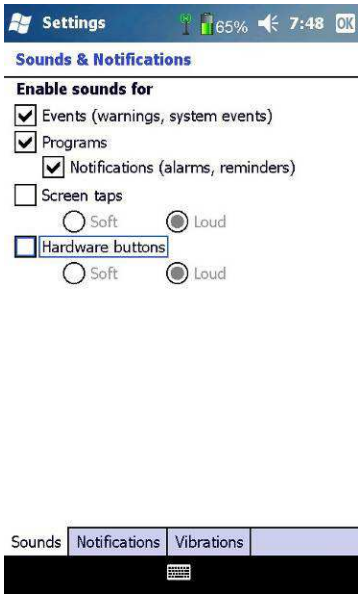
Configuring Data Input Method

- By default, Keyboard Emulation is selected.
- If "Serial Port" option is selected, data will sent to COM9. The port settings is 9600,N,8,1.
- Prefix/Suffix are characters added to scanning result beginning and ending. By default, suffix is \r, i.e. newline.
- "Read SN" retrieves S/N of the internal scanning module.
  Note: WF43BS1 S/N should refer to the label affix on the barcode scanner rear instead of this internal S/N.
- Press "Apply Default Settings" could restore scanning engine parameters for proper communication between PDA & the engine.

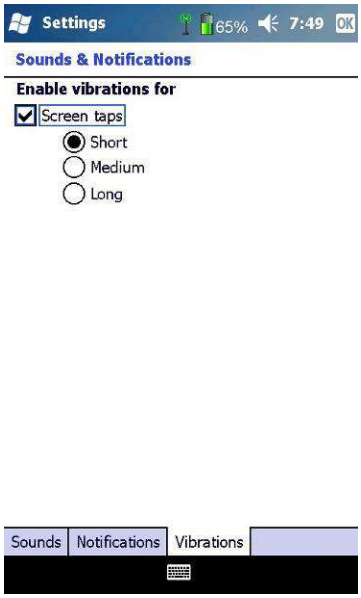
Chapter 14: Misc. Configurations

14.1 Sounds & Notifications

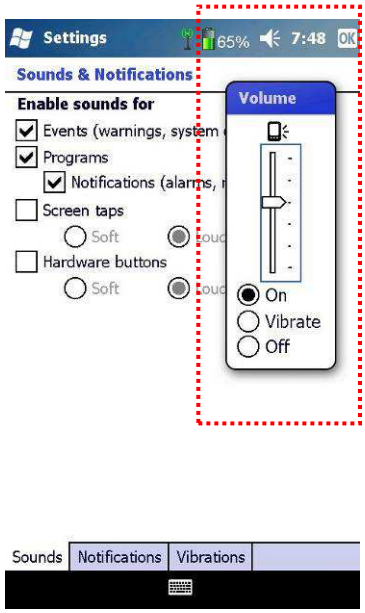
Tap **Start > Settings > Others > Sounds & Notifications**



- By default, screen taps and shortcut keys have no sound



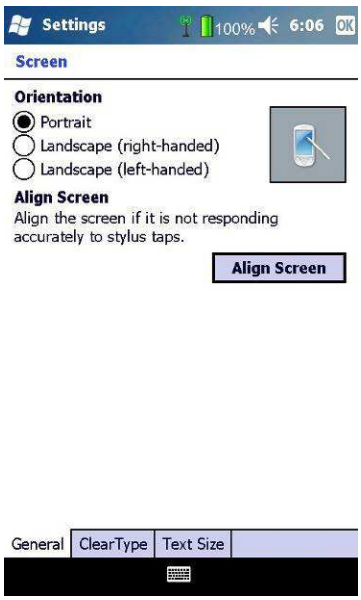
- At page "Vibrations", adjust screen tap vibration strength



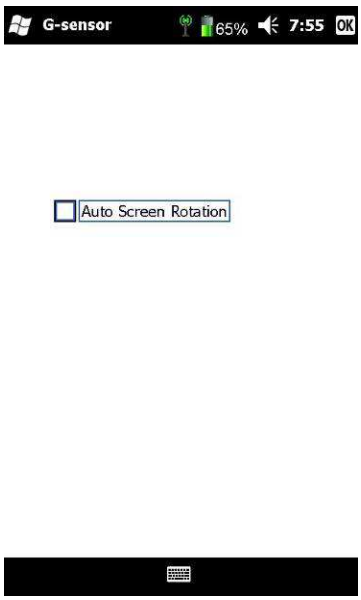
- To adjust the speaker volume, tap speaker icon and apply changes

14.2 Display & Rotation

Tap **Start > Settings > Screen** and **Start > Settings > Others > Auto Rotation**



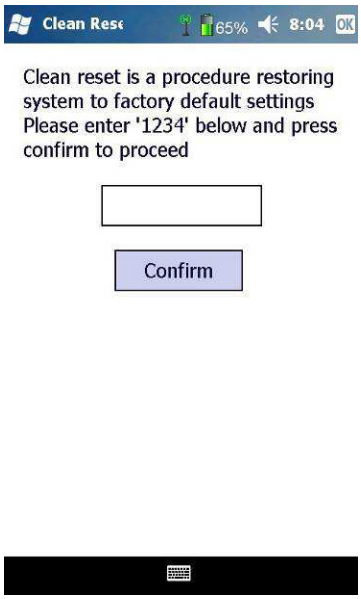
- Configure Portrait or Landscape



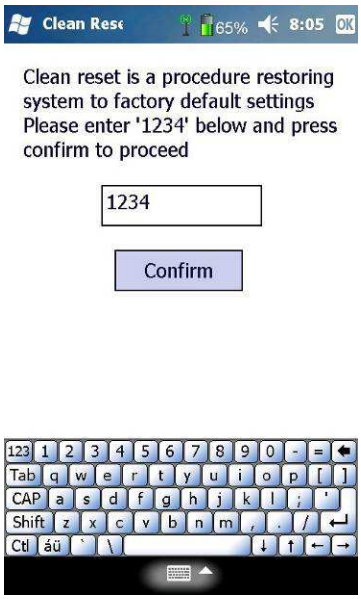
- Configure if screen auto rotation is enabled. It is disabled by default

14.3 Clean Reset

To perform Clean Reset initiated from Windows Mobile environment, tap **Start > Settings > Others > Clean Reset**.



- Clean reset screen

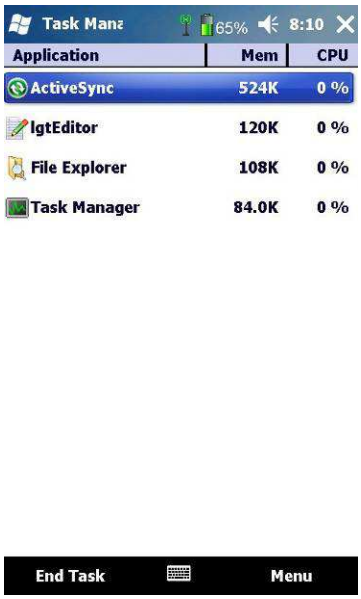


- Enter 1234

- Press "OK" to confirm and reboot. This will initiate clean reset procedure

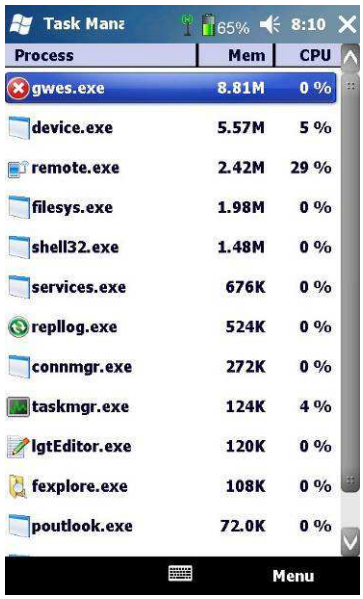
14.4 Task Manager

Task Manager is a system utility that lists out active applications as well as allows killing of unresponsive applications. Tap **Start > Task Manager**.



- Task Manager lists all active applications. Press "End Task" to terminate the selected application.

- To list system processes, press "Menu > View > Processes"



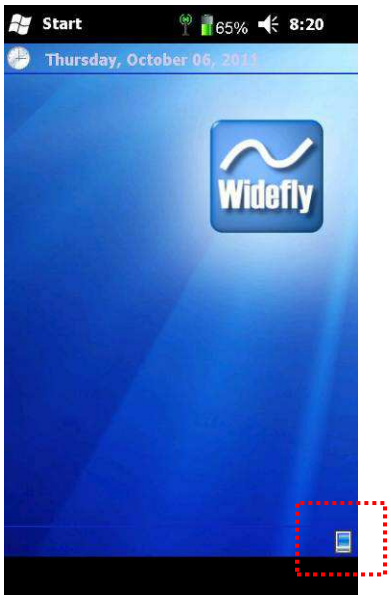
- To list system processes, press "Menu > View > Processes"

Chapter 15: Remote Screen Capture & File Transfer

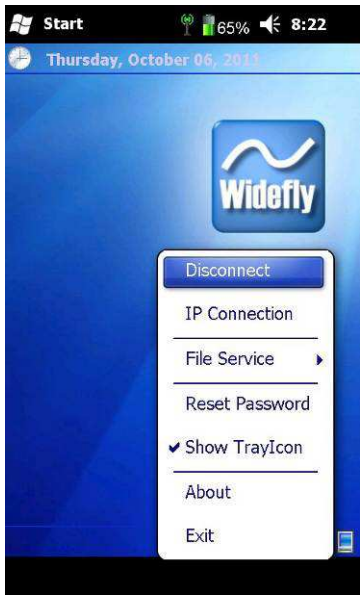
15.1 Remote Display and Screen Capture

A remote display and screen capture utility, call MyMobiler, is pre-installed on the PDA. Tap **Start > Tools > MyMobiler**. Please refer to Chapter 17 – License Info.

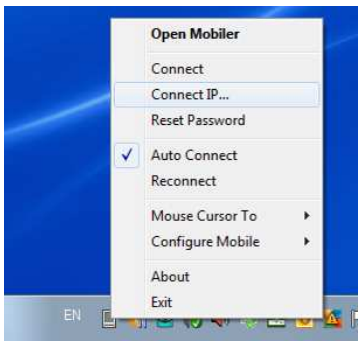
- Start > Tools > MyMobiler
- By default, MyMobiler is not configured to run on boot up



- At today screen, lower right is the MyMobiler agent icon

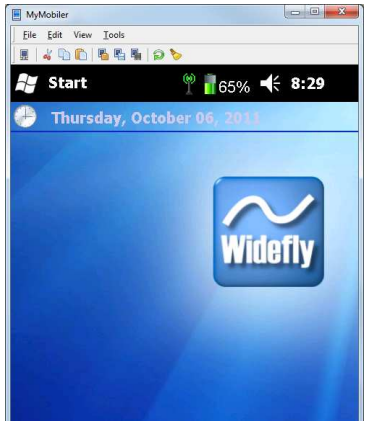


- Tap MyMobiler icon to pop up the configuration menu



- At PC, run MyMobiler program
- Right click the icon and press "Connect IP"

- Enter the IP address of the PDA and press "Connect"



- Remote display and control of PDA enabled
- The screen could be captured in clipboard or saved in file

Note: MyMobiler could be downloaded at http://mymobiler.com/?p=72

15.2 Remote File Transfer

MyMobiler is also a tiny FTP server. When it is executed and stayed resident on the PDA, it allows incoming FTP client connections for file upload & download.

By default, username and password are "admin" and "hello" respectively.

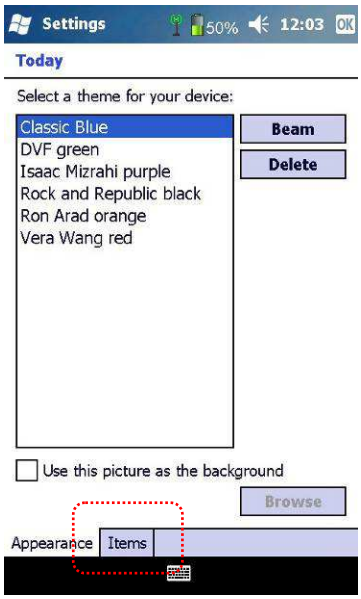
At PC, it is highly recommended to use standard FTP client like FileZilla (http://filezilla-project.org/).

Chapter 16: Configuring Today Screen

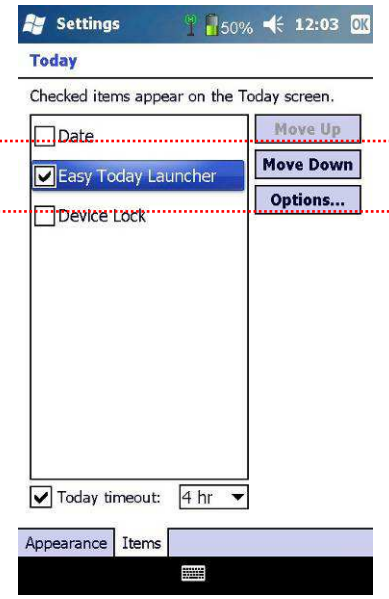
16.1 Create RDP shortcut on Today Screen

The following is an example to place a RDP shortcut on the today screen. Thus, it will be very intuitive to start a RDP by tapping the icon on the today screen as if it is running local application. Follow the steps below after a RDP profile is created.

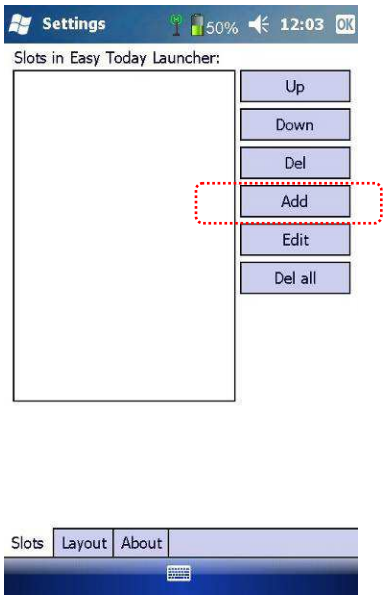
- Goto **Start > Settings > Others > Today**



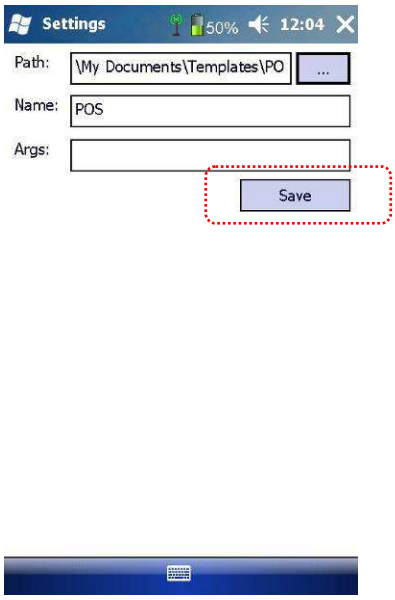
- Tap "Items"



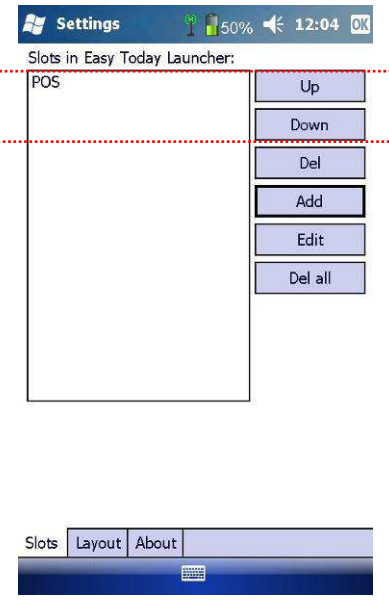
- Uncheck all items except "Easy Today Launcher" and press "Options"



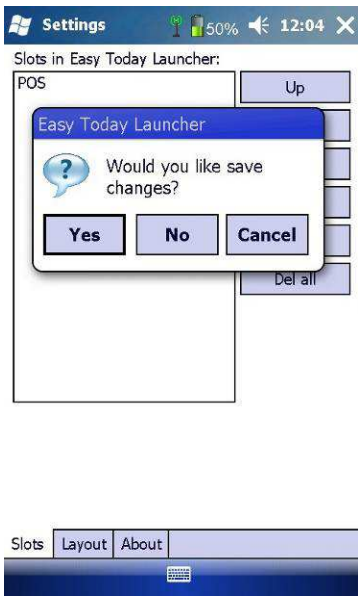
- Press "Add"



- Select folder & RDP profile file
- Press "Save"



- Today screen shortcut "POS" is created and press "OK"

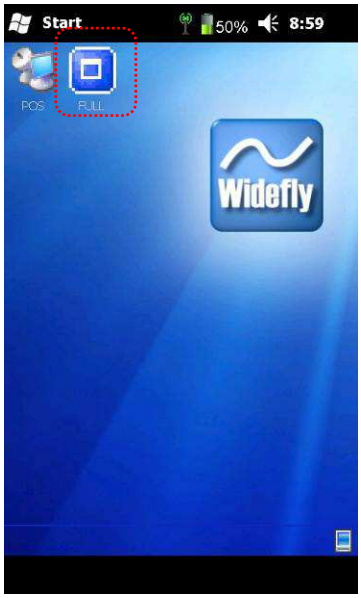


- Press "Yes" to save changes

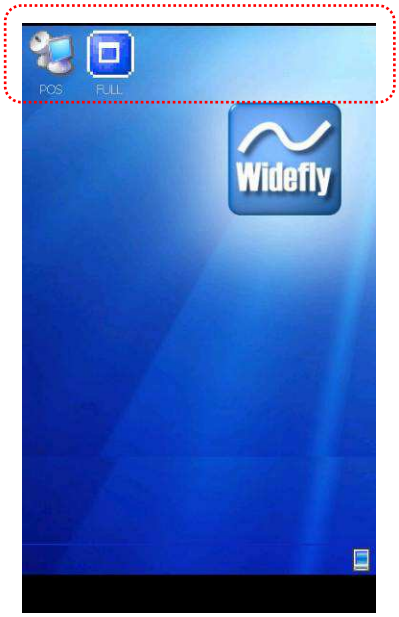
- RDP profile shortcut created on Today Screen.
- End users simply tap this icon to start a RDP session as if running a local application

16.2 Hide and Show Taskbar

The top taskbar could be hidden by a small utility called ToggleStart.exe.



- To hide taskbar, put the ToggleStart.exe on Today Screen



- The ToggleStart utility could hide and show the top taskbar

Note: Easy Today Launcher and ToggleStart.exe is a freeware. Please refer to Chapter 17 - FTP Download for download info.

Chapter 17: FTP Download

17.1 Introduction

Widefly's FTP server provides ROM updates, utilities and sample source codes for downloads.

The FTP logon information is shown below:

Server: ftp.widefly.com

Username: ftp-widefly.wf43

Password: widefly.com.wf43.2011

Folder root: /ftp-widefly.wf43/WF43

17.2 FTP Folders & Files

The following are files & folder structure of the FTP server.

Folder & Files
WF43 ROM /ftp-widefly.wf43/WF43/ROM/ v1.0.2/ v1.0.1 ROM vx.y.z/ vx.y.z ROM (for example) **SDK (Bixolon Bluetooth Printer)** /ftp-widefly.wf43/WF43/SDK/Bixolon Printer Mobile Unified Utility V2.2.0/ Printer setup utility for WM & PC SPP-R200 Windows SDK 1.1.5_STD/ SDK source codes **SDK (WF43MSR)** /ftp-widefly.wf43/WF43/SDK/WF43MSR Source Code for decryption **SDK (Windows Mobile 6.5 SDK for WF43)** /ftp-widefly.wf43/WF43/SDK/WM6.5 – WF43 **Utility** widefly.wf43/WF43/Utility Bixolon Printer/ Bixolon Printer test utility WF43MSR/ WF43MSR configuration utility Freeware/ Windows Mobile freeware (ToggleStart, Easy Today Launcher, MyMobiler)

Chapter 18: License Info

18.1 Freeware

License Info
Easy Today Launcher v1.1.0.3 is a freeware from Loffactory Website: http://loffactory.webs.com/easytodaylauncher.htm lgtEditor v2.0 is a freeware from Fann Software http://www.fannsoftware.com/PpcSoftMain.html MyMobiler v1.25 is a freeware from MyMobiler http://www.mymobiler.com/

<< End of document >>